HYPERELLIPTIC JACOBIANS WITH REAL MULTIPLICATION

ARSEN ELKIN

ABSTRACT. Let K be a field of characteristic $p \neq 2$, and let $f(x)$ be a sextic polynomial irreducible over K with no repeated roots, whose Galois group is isomorphic to $\mathbb{A}_5$. If the jacobian $J(C)$ of the hyperelliptic curve $C : y^2 = f(x)$ admits real multiplication over the ground field from an order of a real quadratic field D, then either its endomorphism algebra is isomorphic to D, or $p > 0$ and $J(C)$ is a supersingular abelian variety. The supersingular outcome cannot occur when p splits in D.

1. Statement of Results

Let K be a field and let K_a be its fixed algebraic closure. Let $f(x) \in K[x]$ be an irreducible polynomial of degree $n = 6$ with no repeated roots. Denote by $\mathfrak{R}_f \subset K_a$ the set of roots of f and by $K(\mathfrak{R}_f)$ the extension of K generated by the elements of $\mathfrak{R}_f$, that is, the splitting field of f over K. We write $\mathrm{Gal}(f/K)$ for the Galois group of $K(\mathfrak{R}_f)/K$, or simply $\mathrm{Gal}(f)$ when no confusion over the ground field arises. This group acts on the elements of $\mathfrak{R}_f$ by permutations, and it is well-known that this action is transitive if and only if f is irreducible over K.

Consider the hyperelliptic curve defined over K by

$$C_f : y^2 = f(x).$$

Let $J(C_f)$ be its jacobian, $\mathrm{End}(J(C_f))$ the ring of K_a-endomorphisms of $J(C_f)$, and $\mathrm{End}_K(J(C_f))$ the ring of K-endomorphisms of $J(C_f)$. We define algebras $\mathrm{End}^0(J(C_f)) := \mathrm{End}(J(C_f)) \otimes \mathbb{Q}$ and $\mathrm{End}^0_K(J(C_f)) := \mathrm{End}_K(J(C_f)) \otimes \mathbb{Q}$. One may view $\mathrm{End}(J(C_f))$ and $\mathrm{End}_K(J(C_f))$ as orders in the corresponding $\mathbb{Q}$-algebras.

For every algebraic curve C, the ring $\mathrm{End}(J(C))$ contains the multiplications by integers; that is, $\mathbb{Z}\cdot\mathrm{Id}_{J(C)} \subset \mathrm{End}(J(C))$, where $\mathrm{Id}_{J(C)}$ is the identity automorphism of $J(C)$. Examples with the precise equality $\mathrm{End}(J(C)) = \mathbb{Z}$ are harder to find (see [10, 11, 12]). In [26, 29, 30] Yu. Zarhin proves that if $\mathrm{Gal}(f)$ is isomorphic to either $\mathbb{A}_n$ or $\mathbb{S}_n$, then this equality holds for the curve C_f, or $\mathrm{char}(K) = 3$, $n = 5$ or 6, and $J(C_f)$ is a supersingular abelian variety. In [28] he proves that if the roots $\mathfrak{R}_f$ of a polynomial f can be identified with $\mathbb{P}^{m-1}(\mathbb{F}_q)$ for some odd prime power q and integer $m > 2$, and $\mathrm{Gal}(f)$ contains $\mathrm{PSL}_m(\mathbb{F}_q)$ as a subgroup, then $\mathrm{End}(J(C_f)) = \mathbb{Z}$ or $J(C_f)$ is a supersingular abelian variety. This statement is not necessarily true for $m = 2$.

Similarly, examples of hyperelliptic curves C_f with $\mathrm{End}(J(C_f))$ containing an order of a real quadratic field (admitting real multiplication) are known (see [23, 24]). The purpose of this paper is to provide a tool for construction of explicit

Date: February 1, 2008.

2000 *Mathematics Subject Classification.* Primary: 14H40 Secondary: 11G10.

Key words and phrases. algebraic geometry, hyperelliptic curves, real multiplication, jacobian varieties, supersingular.

examples of hyperelliptic curves C_f for which $\mathrm{End}(J(C_f))$ is isomorphic to the ring of integers of a real quadratic field $D = \mathbb{Q}(\omega)$, where $\omega^2 = d$ for some square-free integer $d \geq 2$ called the *reduced discriminant* of D. Simply put, $\omega = \sqrt{d}$. Consider polynomials f of degree $n = 6$, in which case curves C_f have genus $g = 2$. We will denote the discriminant of an algebraic number field D (or its order $\mathcal{O}$) by $\delta(D)$ (respectively $\delta(\mathcal{O})$) . We fix all of the above notation throughout the paper.

We will prove the following statement.

Theorem 1.1 (The Main Theorem)**.** *Let K be a field of characteristic $p \neq 2$. Let $f(x) \in K[x]$ be an irreducible separable polynomial of degree $n = 6$. Let $J(C_f)$ be the jacobian of the hyperelliptic curve $C_f : y^2 = f(x)$. Let D be a real quadratic field. Assume that $\mathrm{Gal}(f)$ and $J(C_f)$ enjoy the following properties:*

(a) $\mathrm{Gal}(f) \cong \mathbb{A}_5$,
(b) *there exists an injective ring homomorphism $i : D \hookrightarrow \mathrm{End}^0_K(J(C_f))$ such that $i(1) = \mathrm{Id}_{J(C_f)}$, the identity automorphism of $J(C_f)$.*

Then $\mathrm{End}_K(J(C_f))$ is isomorphic to an order of D with

$$\delta(\mathrm{End}_K(J(C_f))) \equiv 5 \bmod 8,$$

and one of the following conditions holds:

(i) *$J(C_f)$ is an absolutely simple abelian variety and*
$$\mathrm{End}(J(C_f)) = \mathrm{End}_K(J(C_f)).$$
(ii) *$p > 0$ and $J(C_f)$ is a supersingular abelian variety. Moreover, p does not split in D.*

This theorem is a modification of the results in [26, 29, 30]. The structure of the paper is as follows. The proof of Theorem 1.1 will be given in Section 2. In Section 7, the impossibility of the supersingular outcome when $p = \mathrm{char}(K)$ splits in D is proven. Examples in characteristic zero will be given in Section 8. Examples, both supersingular and not, in positive characteristic will be given in Section 9.

Remark 1.2. If $\mathcal{O}$ is an order of $D = \mathbb{Q}(\omega)$ with conductor c (see Section 2), then the condition $\delta(\mathcal{O}) \equiv 5 \bmod 8$ is equivalent to $d \equiv 5 \bmod 8$ and c being odd.

Remark 1.3. If D is a quadratic field with reduced discriminant d, then in order for an odd rational prime p not to split in D it is necessary and sufficient that either $p|d$ (in which case, p ramifies in D) or $\left(\frac{d}{p}\right) = -1$ (that is, p is inert in D).

Remark 1.4. Since f is irreducible over K, the action of $\mathrm{Gal}(f)$ on the set $\mathfrak{R}_f$ on the roots of f is transitive. According to [4, Table. 2.1, p. 60], the six roots of an irreducible polynomial f with $\mathrm{Gal}(f) \cong \mathbb{A}_5$ can be identified with the elements of $\mathbb{P}^1(\mathbb{F}_5)$ in such a way that the action of $\mathrm{Gal}(f)$ on the set $\mathfrak{R}_f$ is isomorphic to the action of $\mathrm{PSL}_2(\mathbb{F}_5) \cong \mathbb{A}_5$ on $\mathbb{P}^1(\mathbb{F}_5)$. Note that this action is doubly transitive.

In proving Theorem 1.1 we will use the following statement, whose proof will be given in Section 4.

Theorem 1.5. *Let K be a field of characteristic different from 2. Let $f(x) \in K[x]$ be an irreducible separable polynomials of degree $n = 6$ with $\mathrm{Gal}(f) \cong \mathbb{A}_5$. Let $X = J(C_f)$ be the jacobian of the hyperelliptic curve $C_f : y^2 = f(x)$. Let R be a subalgebra of $\mathrm{End}_{\mathbb{F}_2}(X_2)$ containing the identity automorphism of X_2 such that*

$${}^{\sigma}u \in R \quad \textit{for each } u \in R, \sigma \in \mathrm{Gal}(K),$$

where

$$^{\sigma}u : x \mapsto \sigma u(\sigma^{-1}x), \quad x \in X_2.$$

Then $\mathrm{End}_{\mathrm{Gal}(K)}(X_2) \cong \mathbb{F}_4$ *and one of the following* $\mathbb{F}_2$*-algebra isomorphisms holds:*

(i) $R \cong \mathbb{F}_2$.
(ii) $R \cong \mathbb{F}_4$.
(iii) $R \cong \mathrm{Mat}_2(\mathbb{F}_4)$.
(iv) $R = \mathrm{End}_{\mathbb{F}_2}(X_2) \cong \mathrm{Mat}_4(\mathbb{F}_2)$.

As a corollary to this theorem we will also obtain

Theorem 1.6. *Let K be a field of characteristic different from 2. Let $f(x) \in K[x]$ be an irreducible separable polynomial of degree $n = 6$ with* $\mathrm{Gal}(f) \cong \mathbb{A}_5$. *Let $C_f : y^2 = f(x)$ be a hyperelliptic curve over K. Then either*

(a) $\mathrm{End}_K(J(C_f)) = \mathbb{Z}$, *or*
(b) $\mathrm{End}_K(J(C_f))$ *is isomorphic to an order of a quadratic field with*

$$\delta(\mathrm{End}_K(J(C_f))) \equiv 5 \bmod 8.$$

The proof of this theorem will be given in Section 2.

The following statement will be used in order to show that jacobians we produce as examples in Section 8 are pairwise non-isogenous. Its proof will be given in Section 5.

Theorem 1.7. *Let K be a field of characteristic 0, $f(x), h(x) \in K(x)$ irreducible separable polynomials over K of degree $n = 6$ each, such that $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ are linearly disjoint extensions of K. Assume that $J(C_f)$ and $J(C_h)$ satisfy the conditions of Theorem 1.1. Then*

$$\mathrm{Hom}(J(C_f), J(C_h)) = 0 \quad \textit{and} \quad \mathrm{Hom}(J(C_h), J(C_f)) = 0.$$

2. Proof of the Main Result

For an abelian variety X defined over a field of characteristic distinct from 2, the natural action of $\mathrm{End}(X)$ on X_2 induces an injective homomorphism

$$\mathrm{End}(X) \otimes \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{End}(X_2).$$

By [18, p. 501] we have $\mathrm{End}_K(X) = \mathrm{End}^0_K(X) \cap \mathrm{End}(X)$, so the map

$$\mathrm{End}_K(X) \otimes \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{End}(X_2)$$

is also an injection (see [14, p. 177]). The image of this homomorphism lies in $\mathrm{End}_{\mathrm{Gal}(K)}(X_2)$.

Before we continue, let us prove the following useful statement, which explains why the discriminants of orders considered in this paper have to belong to a certain congruence class.

Lemma 2.1. *Let D be a $\mathbb{Q}$-algebra that is a 2-dimensional vector space over $\mathbb{Q}$, and let $\mathcal{O}$ be an order of D. Then $\mathbb{F}_2$-algebras $\mathcal{O} \otimes \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{F}_4$ are isomorphic if and only if D is a quadratic field and $\delta(\mathcal{O}) \equiv 5 \bmod 8$.*

Proof. First, we show that if $\mathcal{O} \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_4$ then D is a field. Proceeding by contradiction, assume that for some nonzero $u, v \in D$, we have $uv = 0$. After multiplying u and v by appropriate nonzero rational numbers we can assume that $u, v \in \mathcal{O}$ and neither is divisible by 2 in $\mathcal{O}$. Then the image of neither u nor v in $\mathcal{O} \otimes \mathbb{Z}/2\mathbb{Z}$ equals to 0, but their product does, which leads to a contradiction. Hence

D is a $\mathbb{Q}$-division algebra of dimension 2 as a $\mathbb{Q}$-vector space, or, equivalently, a quadratic field.

Assume D is a quadratic field. Let $d \geq 2$ be the reduced discriminant of D; that is, assume that $D = \mathbb{Q}(\sqrt{d})$ with d square-free. It is well-known that $\mathcal{O} = \mathbb{Z}[c\eta]$, where

$$\eta = \begin{cases} (\sqrt{d}-1)/2 & \text{for } d \equiv 1 \bmod 4, \\ \sqrt{d} & \text{for } d \equiv 2 \text{ or } 3 \bmod 4, \end{cases}$$

and c is a positive integer called the *conductor* of $\mathcal{O}$. The minimal polynomial of the generator $c\eta$ is

$$g(X) = \begin{cases} X^2 + cX - c^2(d-1)/4 & \text{for } d \equiv 1 \bmod 4, \\ X^2 - c^2 d & \text{for } d \equiv 2 \text{ or } 3 \bmod 4. \end{cases}$$

The field $\mathbb{F}_4$ is the splitting field of $X^2 + X + 1$ over $\mathbb{F}_2$, the only irreducible polynomial of degree 2 over $\mathbb{F}_2$. We have $\mathbb{Z}[c\eta] \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_4$ if and only if the minimal polynomial of $c\eta$ is congruent to $X^2 + X + 1$ modulo 2. This happens if and only if $d \equiv 5 \bmod 8$ and $c \equiv 1 \bmod 2$. It is easy to see that this is equivalent to $\delta(\mathcal{O}) \equiv 5 \bmod 8$. □

As an application of this lemma we obtain:

Proof of Theorem 1.6. Let K, f, C_f, and $X = J(C_f)$ be as in Theorem 1.6. By Theorem 1.5, $\mathrm{End}_{\mathrm{Gal}(K)}(X_2) \cong \mathbb{F}_4$. Hence $\mathrm{End}_K(X) \otimes \mathbb{Z}/2\mathbb{Z} \subset \mathbb{F}_4$, and $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}_K(X)) \leq 2$. Rank of the free $\mathbb{Z}$-module $\mathrm{End}_K(X)$ and dimension of $\mathbb{Q}$-algebra $\mathrm{End}^0_K(X)$ are equal to the $\mathbb{F}_2$-dimension of the algebra $\mathrm{End}_K(X) \otimes \mathbb{Z}/2\mathbb{Z}$. So if $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}_K(X)) = 1$ then $\mathrm{End}_K(X)) = \mathbb{Z}$.

If $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}_K(X)) = 2$ then the $\mathbb{Q}$-algebra $\mathrm{End}^0_K(X)$ has dimension 2 as a $\mathbb{Q}$-vector space. It is well-known that $\mathrm{End}_K(X)$ is isomorphic to an order of $\mathrm{End}^0_K(X)$ and by Lemma 2.1, we have D is a quadratic field and

$$\delta(\mathrm{End}_K(X)) \equiv 5 \bmod 8.$$

□

Proof of Theorem 1.1. Let $C = C_f$ be the hyperelliptic curve defined over K by the equation $y^2 = f(x)$ such that all conditions of Theorem 1.1 hold for the polynomial f and abelian variety $X = J(C)$.

We know that $\mathrm{End}_K(X)$ contains the order $i(D) \cap \mathrm{End}(X)$ of $i(D)$, whose $\mathbb{Z}$-rank is 2. Therefore, $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}_K(X)) = 2$ and, by Theorem 1.6, $\mathrm{End}_K(X)$ is isomorphic to an order of D.

Let us consider the possible options for the $\mathrm{Gal}(K)$-stable algebra

$$R := \mathrm{End}(X) \otimes \mathbb{Z}/2\mathbb{Z} \subset \mathrm{End}_{\mathbb{F}_2}(X_2)$$

which are provided by Theorem 1.5. First, note that the rank of the free $\mathbb{Z}$-module $\mathrm{End}(X)$ and dimension of $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$ are equal to the $\mathbb{F}_2$-dimension of the algebra $\mathrm{End}(X) \otimes \mathbb{Z}/2\mathbb{Z}$.

Case (i): $\mathrm{End}(X) \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$. This case cannot occur, since the rank of $\mathrm{End}(X)$, which contains $\mathrm{End}_K(X)$, is at least 2.

Case (ii): $\mathrm{End}(X) \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_4$. In this case, the free $\mathbb{Z}$-module $\mathrm{End}(X)$ has rank 2, and the ring $\mathrm{End}(X)$ is isomorphic to an order of the real quadratic field $D \cong \mathrm{End}^0_K(X) = \mathrm{End}_K(X) \otimes \mathbb{Q}$. Note that $\mathrm{End}^0(X) \cong D$ is a simple division algebra, so X is not isogenous over the algebraic closure K_a of K to a product of

two elliptic curves. Therefore, X is an absolutely simple abelian variety. In this case, the equality $\mathrm{End}(J(C_f)) = \mathrm{End}_K(J(C_f))$ holds.

Case (iii): $\mathrm{End}(X) \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathrm{Mat}_2(\mathbb{F}_4)$**.** Then we have $\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) = 8$. In order to eliminate this outcome, let us consider the following possibilities.

(1) It is well-known [16] that if X is an absolutely simple abelian variety of dimension 2, then its endomorphism algebra $\mathrm{End}^0(X)$ is an Albert algebra of type I(1), I(2), II(1), or IV(2, 1), which means that $\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) \neq 8$.

(2) Suppose X is isogenous over K_a to a product of two non-isogenous elliptic curves E_1 and E_2. We have

$$\mathrm{End}^0(X) \cong \mathrm{End}^0(E_1) \oplus \mathrm{End}^0(E_2)$$

and

$$\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) = \dim_{\mathbb{Q}}(\mathrm{End}^0(E_1)) + \dim_{\mathbb{Q}}(\mathrm{End}^0(E_2)).$$

It is well-known [20, pp. 102 and 165], that the endomorphism algebra of an elliptic curve has $\mathbb{Q}$-dimension of 1 or 2 in characteristic 0, and $1, 2$ or 4 in positive characteristic. This means that $\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) \neq 8$, since the equality would imply that E_1 and E_2 are both supersingular and, therefore, isogenous.

(3) If X is isogenous over K_a to a square of an elliptic curve E_1 then

$$\mathrm{End}^0(X) \cong \mathrm{Mat}_2(\mathrm{End}^0(E_1))$$

and

$$\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) = 4 \dim_{\mathbb{Q}}(\mathrm{End}^0(E_1)).$$

and for this dimension over $\mathbb{Q}$ to be 8, we must have $\dim_{\mathbb{Q}}(\mathrm{End}^0(E_1)) = 2$. This means that $\mathrm{End}^0(X)$ is a matrix algebra of size 2 over an imaginary quadratic extension $L = \mathrm{End}^0(E_1)$ of $\mathbb{Q}$. The order $\mathcal{L} = L \cap \mathrm{End}(X)$ of the center L of $\mathrm{End}^0(X)$ has the property that $\mathcal{L} \otimes \mathbb{Z}/2\mathbb{Z} \subset \mathrm{End}_{\mathbb{F}_2}(X_2)$ is stable under the adjoint action of the group $\mathrm{Gal}(K)$.

We know that the ring $\mathrm{End}_K(X)$ has the same property. Note that the subalgebra $\mathrm{End}^0_K(X) = \mathrm{End}_K(X) \otimes \mathbb{Q}$ of $\mathrm{End}^0(X)$ is isomorphic to a real quadratic field, and therefore it does not coincide with the algebra L, to which it is not isomorphic. Hence the compositum $\mathrm{End}^0_K(X)L$ of $\mathrm{End}^0_K(X)$ and L has dimension 4 over $\mathbb{Q}$. It is $\mathrm{Gal}(K)$-stable.

Let $\mathcal{R} = \mathrm{End}^0_K(X)L \cap \mathrm{End}(X)$. The ring $\mathcal{R}$ is an order of $\mathrm{End}^0_K(X)L$ and therefore has rank 4 over $\mathbb{Z}$. According to [14, p. 177], there exists an injective $\mathrm{Gal}(K)$-homomorphism $\mathcal{R} \otimes \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{End}(X_2)$. The image of this homomorphism is also $\mathrm{Gal}(K)$-stable and therefore satisfies all of the conditions of Theorem 1.5. Hence it must fit one of the three possible choices prescribed by this theorem. However, the $\mathbb{F}_2$-dimension of $\mathcal{R}\otimes\mathbb{Z}/2\mathbb{Z}$ is 4, while the dimensions of spaces in Theorem 1.5 are 1, 2, 8, and 16. We arrive at a contradiction.

Case (iv): $\mathrm{End}(X) \otimes \mathbb{Z}/2\mathbb{Z} = \mathrm{End}_{\mathbb{F}_2}(X_2)$**.** The free $\mathbb{Z}$-module $\mathrm{End}(X)$ has rank 16. Recall that $g = \dim(X) = 2$. This implies $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}(X)) = (2g)^2$, and the semisimple $\mathbb{Q}$-algebra $\mathrm{End}^0(X) = \mathrm{End}(X) \otimes \mathbb{Q}$ has dimension $(2g)^2$. This means that $\mathrm{char}(K) > 0$ and X is a supersingular abelian variety (see [26, Lemma 3.1]). $\square$

3. Permutation Groups and Permutation Modules

In proving Theorem 1.5 we will need some basic results about the structure of $J(C)_2$. Let B be a set of even cardinality $n \geq 6$. Denote by $\mathrm{Perm}(B)$ the group of permutations on B. A choice of an ordering on B induces an isomorphism $\mathrm{Perm}(B) \cong \mathbb{S}_n$. Let $\mathbb{F}$ be a field of characteristic 2, and denote by $\mathbb{F}^B$ the n-dimensional $\mathbb{F}$-vector space of maps from B to $\mathbb{F}$. The action of $\mathrm{Perm}(B)$ on B extends to an action of $\mathrm{Perm}(B)$ on $\mathbb{F}^B$ as follows: an element $\sigma \in \mathrm{Perm}(B)$ sends a map $f : B \to \mathbb{F}$ to map $\sigma f : b \mapsto f(\sigma^{-1}(b))$. The subspace

$$(\mathbb{F}^B)^0 = \{f : B \to \mathbb{F} \mid \sum_{b \in B} f(b) = 0\}.$$

of $\mathbb{F}^B$ is stable under the action of $\mathrm{Perm}(B)$. In turn, $\mathrm{Perm}(B)$-module $(\mathbb{F}^B)^0$ contains a stable submodule $\mathbb{F} \cdot 1_B$ of constant functions $B \to \mathbb{F}$. Given a subgroup G of $\mathrm{Perm}(B)$, we define the *heart* of the permutation representation of G on B over $\mathbb{F}$ to be the quotient

$$(\mathbb{F}^B)^{00} = (\mathbb{F}^B)^0/(\mathbb{F} \cdot 1_B).$$

It is easy to show that $(\mathbb{F}^B)^{00}$ is a faithful G-module.

When $\mathbb{F} = \mathbb{F}_2$ we will write Q_B instead of $(\mathbb{F}_2^B)^{00}$. In this case, Q_B can also be described as the set of equivalence classes of subsets of B of even cardinality with symmetric difference as sum where subsets complementary in B are identified.

Lemma 3.1. *Let G be a subgroup of* $\mathrm{Perm}(B)$*. Then we have an $\mathbb{F}_4[G]$-module isomorphism*

$$(\mathbb{F}_4^B)^{00} \cong Q_B \otimes_{\mathbb{F}_2} \mathbb{F}_4$$

and an $\mathbb{F}_4$-algebra isomorphism

$$\mathrm{End}_{G,\mathbb{F}_4}((\mathbb{F}_4^B)^{00}) \cong \mathrm{End}_G(Q_B) \otimes_{\mathbb{F}_2} \mathbb{F}_4.$$

Proof. The first statement is obvious and the second immediately follows from Lemma 10.37 of [3]. □

Let $C_f : y^2 = f(x)$ be a hyperelliptic curve defined over a field K of characteristic different from 2 by an irreducible separable polynomial $f(x) \in K[x]$ of even degree n, and let $\mathfrak{R}$ denote the set of roots of f. It is well-known that the $\mathrm{Gal}(K)$-modules $J(C_f)_2$ and $Q_{\mathfrak{R}}$ are isomorphic.

Now assume that $n = 6$ and $\mathrm{Gal}(f) \cong \mathrm{PSL}_2(\mathbb{F}_5)$. Then $\dim(J(C_f)) = 2$ and $\dim_{\mathbb{F}_2}(J(C_f)_2) = 4$. Let $\overline{\rho}_{2,X} : \mathrm{Gal}(K) \to \mathrm{Aut}(J(C_f)_2)$ be the action of $\mathrm{Gal}(K)$ on $J(C_f)_2$ and let $G = \overline{\rho}_{2,X}(\mathrm{Gal}(K)) \subset \mathrm{Aut}(J(C_f)_2)$ be the image of $\mathrm{Gal}(K)$ under this representation. The action of $\mathrm{Gal}(K)$ on $J(C_f)_2$ factors through G, and the action of $\mathrm{Gal}(K)$ on $\mathfrak{R}$ factors through $\mathrm{Gal}(f)$. We have $G \cong \mathrm{Gal}(f) \cong \mathrm{PSL}_2(\mathbb{F}_5)$ and the faithful G-modules $J(C_f)_2$ and $Q_{\mathfrak{R}}$ are isomorphic.

Lemma 3.2. *$Q_{\mathfrak{R}}$ is a simple G-module.*

Proof. See Table 1 in [13]. □

Lemma 3.3. *The $\mathbb{F}_2$-algebras* $\mathrm{End}_G(Q_{\mathfrak{R}})$ *and $\mathbb{F}_4$ are isomorphic.*

Proof. Since the representation $G \to \mathrm{Aut}_{\mathbb{F}_2}(Q_{\mathfrak{R}})$ is irreducible, by Schur's Lemma $\mathrm{End}_G(Q_{\mathfrak{R}})$ is a division algebra. Since it is finite, it must be a field, which we will denote by $\mathbb{F}$.

According to Table 1 in [13], the G-module $(\mathbb{F}_4^B)^{00}$ is reducible. Therefore, $\mathrm{End}_{G,\mathbb{F}_4}((\mathbb{F}_4^B)^{00}) \cong \mathrm{End}_G(Q_{\mathfrak{R}}) \otimes_{\mathbb{F}_2} \mathbb{F}_4$ is not a field. This means that $\mathbb{F} = \mathrm{End}_G(Q_{\mathfrak{R}})$ contains $\mathbb{F}_4$, a quadratic extension of $\mathbb{F}_2$, as a subfield. Hence $\mathbb{F} \cong \mathbb{F}_{4^s}$ for some positive integer s. The embedding of $\mathbb{F}$ in $\mathrm{End}_{\mathbb{F}_2}(Q_{\mathfrak{R}})$ provides $Q_{\mathfrak{R}}$ with a structure of an $\mathbb{F}$-vector space. Since $\#(Q_{\mathfrak{R}}) = 16$, we must have $\mathbb{F} \cong \mathbb{F}_4$ or $\mathbb{F}_{16}$.

If $\mathbb{F} \cong \mathbb{F}_{16}$ then $Q_{\mathfrak{R}}$ is a 1-dimensional $\mathbb{F}$-vector space, so $\mathrm{End}_{\mathbb{F}}(Q_{\mathfrak{R}}) = \mathbb{F}$. Since $\mathbb{F} = \mathrm{End}_G(Q_{\mathfrak{R}})$, we have $G \subset \mathrm{Aut}_{\mathbb{F}}(Q_{\mathfrak{R}})$ as a subgroup, which is a contradiction. Indeed, the group $\mathrm{Aut}_{\mathbb{F}}(Q_{\mathfrak{R}}) = \mathbb{F}^{\times}$ is abelian, while $G \cong \mathbb{A}_5$ is not. □

In light of the fact that $\mathrm{End}_G(Q_{\mathfrak{R}}) = \mathrm{End}_{\mathrm{Gal}(f)}(J(C)_2) = \mathrm{End}_{\mathrm{Gal}(K)}(J(C)_2)$ this lemma can be restated as

$$\dim_{\mathbb{F}_2} \mathrm{End}_{\mathrm{Gal}(K)}(J(C)_2) = 2,$$

and, since $\mathrm{End}_K(J(C)) \otimes \mathbb{Z}/2\mathbb{Z}$ injectively embeds in $\mathrm{End}_{\mathrm{Gal}(K)}(J(C)_2)$, we get Theorem 1.6.

From Lemmas 3.2 and 3.3, and Theorem 3.43 of [3, p. 54] follows:

Corollary 3.4. *The $\mathbb{F}_4[G]$-module $Q_{\mathfrak{R}}$ is absolutely simple.*

4. Proof of the Auxiliary Theorem

Theorem 1.5 follows immediately from the discussion of the previous section and this theorem:

Theorem 4.1. *Let X be an abelian variety over field K of characteristic different from 2. Let $G = \overline{\rho}_{2,X}(\mathrm{Gal}(K)) \subset \mathrm{End}_{\mathbb{F}_2}(X_2)$. Assume that the following conditions are satisfied:*

(a) $\dim(X) = 2$,
(b) $G \cong \mathbb{A}_5$,
(c) X_2 *is a simple G-module,*
(d) $\mathrm{End}_G(X_2) \cong \mathbb{F}_4$.

Identify $\mathbb{F}_2$ with its embedding $\mathbb{F}_2 \cdot \mathrm{Id}_{X_2} \subset \mathrm{End}(X_2)$, where Id_{X_2} is the identity automorphism of X_2, and identify $\mathbb{F}_4$ with $\mathrm{End}_G(X_2)$. Let R be a subalgebra of $\mathrm{End}_{\mathbb{F}_2}(X_2)$ containing the identity automorphism Id of X_2 such that

$$uRu^{-1} \subset R \quad \text{for all } u \in G.$$

Then we have one of the following cases:

(i) $R = \mathbb{F}_2$;
(ii) $R = \mathbb{F}_4$;
(iii) $R = \mathrm{End}_{\mathbb{F}_4}(X_2)$;
(iv) $R = \mathrm{End}_{\mathbb{F}_2}(X_2)$.

Proof. Since X_2 is a faithful R-module, we have

$$uRu^{-1} = R \quad \text{for all } u \in G \subset \mathrm{Aut}_{\mathbb{F}_2}(X_2).$$

Lemma 4.2. *X_2 is a semisimple R-module.*

Proof. This is a reproduction of a similar proof in [26, of Th. 5.3]. Let $U \in X_2$ be a simple R-submodule. Then $U' = \sum_{s\in G} sU$ is a non-zero G-invariant subspace in X_2, and, since X_2 is a simple G-module, $U' = X_2$. Each sU is also an R-submodule

in X_2, because $s^{-1}Rs = R$ for all $s \in G$. In addition, if $W \subset sU$ is an R-submodule then $s^{-1}W$ is an R-submodule in U, because

$$Rs^{-1}W = s^{-1}sRs^{-1}W = s^{-1}RW = s^{-1}W.$$

Since U is simple, $s^{-1}W = \{0\}$ or U. This implies that sU is also simple. Hence $X_2 = U'$ is a sum of simple R-modules and therefore is a semisimple R-module. $\square$

Lemma 4.3. *The R-module X_2 is isotypic.*

Proof. The proof is a modification of a similar proof [26, of Th. 5.3]. Let

$$X_2 = V_1 \oplus \cdots \oplus V_r$$

be an isotypic decomposition of the semisimple R-module X_2. Looking at the dimensions yields $r \leq \dim_{\mathbb{F}_2}(X_2) = 4$. By repeating the argument in the proof of the previous claim, we can show that for each isotypic component V_i its image sV_i is an isotypic R-submodule for each $s \in G$ and therefore is contained in some V_j. Similarly, $s^{-1}V_j$ is an isotypic submodule containing V_i. Since V_i is the isotypic component, $s^{-1}V_j = V_i$. This means that s permutes the V_i, and, since X_2 is G-simple, G permutes them transitively. This gives a homomorphism $G \to \mathbb{S}_r$ which must be injective or trivial, since G is simple. However $G \cong \mathbb{A}_5$ and $r \leq 4$, so it is trivial. This means that $sV_i = V_i$ for all $s \in G$ and $X_2 = V_i$ is isotypic. $\square$

From this lemma it follows that there exists a simple R-module W and a positive integer d such that $X_2 \cong W^d$.

We have

$$d \cdot \dim_{\mathbb{F}_2}(W) = \dim_{\mathbb{F}_2}(X_2) = 4.$$

Thus $d = 1, 2$, or 4.

Clearly, $\mathrm{End}_R(X_2)$ is isomorphic to the matrix algebra $\mathrm{Mat}_d(\mathrm{End}_R(W))$. Let us put

$$k = \mathrm{End}_R(W).$$

Since W is simple, k is a finite division algebra of characteristic 2. Hence k is a finite field of characteristic 2, and

$$\mathrm{End}_R(X_2) \cong \mathrm{Mat}_d(k).$$

We have $\mathrm{End}_R(X_2) \subset \mathrm{End}_{\mathbb{F}_2}(X_2)$ is invariant under the adjoint action of G, since R is invariant under adjoint action of G. This induces a homomorphism

$$\alpha : G \to \mathrm{Aut}(\mathrm{End}_R(X_2)) = \mathrm{Aut}(\mathrm{Mat}_d(k)).$$

Since k is the center of $\mathrm{Mat}_d(k)$, it is invariant under the action of G; that is, we get a homomorphism $G \to \mathrm{Aut}(k)$, which must be trivial, since G is a simple group and $\mathrm{Aut}(k)$ is abelian. This implies that the center k of $\mathrm{End}_R(X_2)$ commutes with G and must be a subalgebra of $\mathrm{End}_G(X_2)$. Since $\mathrm{End}_G(X_2) = \mathbb{F}_4$ as an $\mathbb{F}_2$-algebra, we have $k = \mathbb{F}_2$ or $\mathbb{F}_4$.

It follows from the Jacobson density theorem (combined with dimension arguments) that $R \cong \mathrm{Mat}_m(k)$ with $dm = 4$ if $k = \mathbb{F}_2$ and $2dm = 4$ if $k = \mathbb{F}_4$.

Let us rule out the case not mentioned in the outcomes of this theorem: if $R \cong \mathrm{Mat}_2(\mathbb{F}_2)$, the group G acts on $\mathrm{Mat}_2(\mathbb{F}_2)$; that is, we have a homomorphism

$$G \to \mathrm{Aut}(\mathrm{Mat}_2(\mathbb{F}_2)) = \mathrm{PGL}_2(\mathbb{F}_2) \cong \mathrm{GL}_2(\mathbb{F}_2),$$

where the equality follows from the Skolem-Noether theorem. This homomorphism must be trivial, since G is perfect and $\mathrm{GL}_2(\mathbb{F}_2)$ is solvable. Therefore, R commutes with G and is a subalgebra of $\mathrm{End}_G(X_2) = \mathbb{F}_4$. This is a contradiction.

Finally, notice that if $k = \mathrm{End}_G(X_2) = \mathbb{F}_4$, and $R = \mathrm{Mat}_2(k)$, then R commutes with $\mathbb{F}_4$, and therefore lies in $\mathrm{End}_{\mathbb{F}_4}(X_2)$. However, since X_2 is a 2-dimensional $\mathbb{F}_4$-vector space, $\mathrm{End}_{\mathbb{F}_4}(X_2) \cong \mathrm{Mat}_2(\mathbb{F}_4)$, so $R = \mathrm{End}_{\mathbb{F}_4}(X_2)$. $\square$

In [27], Yu. Zarhin makes the following definition.

Definition 4.4. Let V be a vector space over a field k, let G be a group and $\rho : G \to \mathrm{Aut}_k(V)$ a linear representation of G in V. We say that the G-module V is *very simple* if it enjoys the following property:

If $R \subset \mathrm{End}_k(V)$ is a k-subalgebra containing the identity operator Id such that

$$\rho(\sigma) R \rho(\sigma)^{-1} \subset R \quad \text{for all } \sigma \in G$$

then either $R = k \cdot \mathrm{Id}_V$ or $R = \mathrm{End}_k(V)$.

We immediately obtain the following proposition, which will be used in the proof of Theorem 7.2.

Corollary 4.5. *Let X be an abelian variety satisfying the conditions of Theorem 4.1. Then X_2 is a very simple G-module over $\mathbb{F}_4$.*

Proof. The only outcomes of Theorem 4.1 that contain $\mathbb{F}_4$ in the center are $R \cong \mathbb{F}_4$ and $R = \mathrm{End}_{\mathbb{F}_4}(X_2)$. $\square$

5. Non-Isogenous Jacobians

Let us now restate some of the above results in terms of $J(C)_2$ and $\mathrm{Gal}(f)$. If we compose the canonical epimorphism $\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(f)$ with the irreducible representation $\mathrm{Gal}(f) \to \mathrm{Aut}_{\mathbb{F}_2}(J(C)_2)$ of Lemma 3.2 we get

Lemma 5.1. *$J(C)_2$ is a simple $\mathrm{Gal}(K)$-module.*

Note that Corollary 3.4 can be restated as follows:

Corollary 5.2. *Assume that all of the conditions of Theorem 1.1 hold. Then $J(C_f)_2$ is an absolutely simple $\mathbb{F}_4[\mathrm{Gal}(f)]$-module.*

Proof of Theorem 1.7. We prove this theorem by contradiction. Let $X = J(C_f)$ and $Y = J(C_h)$ be abelian varieties in question and assume there exists a nonzero homomorphism $\phi \in \mathrm{Hom}(X, Y)$. Then ϕ is an isogeny.

We can also assume that $X_2 \not\subseteq \ker \phi$. If that is not the case, then ϕ is a composition of multiplication by 2 on X and another isogeny from X to Y, which we can choose instead, continuing this process until the obtained isogeny no longer annihilates X_2.

For every $\psi \in \mathrm{Hom}(X, Y)$ and $\sigma \in \mathrm{Gal}(K)$ we define a homomorphism ${}^{\sigma}\psi \in \mathrm{Hom}(X, Y)$ by ${}^{\sigma}\psi(x) = \sigma\psi(\sigma^{-1}x)$ for all $x \in X(K_a)$. We then define $c : \mathrm{Gal}(K) \to \mathrm{End}^0(X)^{\times}$ by $c_\sigma = \phi^{-1}\, {}^{\sigma}\phi$. It is easy to show that c satisfies the cocycle condition $c_{\sigma\tau} = c_\sigma\, {}^{\sigma}c_\tau$. In addition, we have $\mathrm{End}^0(X) = \mathrm{End}^0_K(X)$, so ${}^{\sigma}c_\tau = c_\tau$ and c is a homomorphism. There exists a finite normal extension K_ϕ of K such that ϕ is defined over K_ϕ. Since we are in characteristic 0, K_ϕ is also Galois over K, so there exists a homomorphism $c' : \mathrm{Gal}(K_\phi/K) \to \mathrm{End}^0(X)^{\times}$ such that c is a composition of the canonical homomorphism $\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(K_\phi/K)$ and c'. Since $\mathrm{Gal}(K_\phi/K)$

is finite, its image under c' in $\operatorname{End}^0(X)^\times$, which coincides with the image of $\operatorname{Gal}(K)$ under c, is also finite. Therefore, this image is either $\{\operatorname{Id}_X\}$ or $\mu_2 = \{\pm \operatorname{Id}_X\}$.

If $c(\operatorname{Gal}(K)) = c'(\operatorname{Gal}(K_\phi/K)) = \mu_2$, let $H = \ker(c')$, and let K' be the subfield of elements of K_ϕ that are fixed by H. Then K' is Galois over K, $\operatorname{Gal}(K_\phi/K') = H$ and $\operatorname{Gal}(K'/K) \cong G/H = \mu_2$. By the choice of H, the image of $\operatorname{Gal}(K_\phi/K')$ under c' is trivial. Therefore, the image of $\operatorname{Gal}(K') \subset \operatorname{Gal}(K)$ under c is trivial. Moreover, since the Galois groups of f and h are perfect and $\operatorname{Gal}(K'/K) \cong \mu_2$ is cyclic, polynomials f and h will be irreducible over K', their Galois groups over K' will still be isomorphic to $\mathbb{A}_5$, and they will still satisfy the conditions of Theorem 1.7. Without loss of generality, we can choose to work over K' instead of K, which reduces the theorem to the next case.

If $c(\operatorname{Gal}(K)) = \{\operatorname{Id}_X\}$ then ϕ is defined over K and commutes with the action of $\operatorname{Gal}(K)$ on X and Y. This remains true if we consider points of order dividing 2: the homomorphism $\varphi = \phi|_{X_2} : X_2 \to Y_2$ commutes with the action of $\operatorname{Gal}(K)$ on X_2 and Y_2. The kernel of φ is a $\operatorname{Gal}(K)$-stable submodule of X_2. Since X_2 is a simple $\operatorname{Gal}(K)$-module, the map φ is either zero or is a $\operatorname{Gal}(K)$-isomorphism. It cannot be zero by the choice of ϕ. We claim that it cannot be an isomorphism either.

Let $L = K(\mathfrak{R}_f \cup \mathfrak{R}_h)$ be the compositum of the splitting fields $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ of f and h and consider the canonical restriction maps $\operatorname{res}^L_{K(\mathfrak{R}_f)} : \operatorname{Gal}(L/K) \to \operatorname{Gal}(f/K)$ and $\operatorname{res}^L_{K(\mathfrak{R}_h)} : \operatorname{Gal}(L/K) \to \operatorname{Gal}(h/K)$. Recall that the $\operatorname{Gal}(f/K)$-module X_2 and $\operatorname{Gal}(h/K)$-module Y_2 are faithful and let $\alpha_X : \operatorname{Gal}(f/K) \hookrightarrow \operatorname{Aut}(X_2)$ and $\alpha_Y : \operatorname{Gal}(h/K) \hookrightarrow \operatorname{Aut}(X_2)$ be the corresponding embeddings. The actions of $\operatorname{Gal}(K)$ on X_2 and Y_2 factor through the canonical epimorphism $\operatorname{res}_L : \operatorname{Gal}(K) \twoheadrightarrow \operatorname{Gal}(L/K)$, that is,

$$\overline{\rho}_{2,X} = \alpha_X \circ \operatorname{res}^L_{K(\mathfrak{R}_f)} \circ \operatorname{res}_L \quad \text{and} \quad \overline{\rho}_{2,Y} = \alpha_Y \circ \operatorname{res}^L_{K(\mathfrak{R}_h)} \circ \operatorname{res}_L .$$

If $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ are linearly disjoint over K, then

$$\operatorname{Gal}(L/K) \cong \operatorname{Gal}(f/K) \times \operatorname{Gal}(h/K),$$

with projections onto each summand coinciding with the Galois restriction maps $\operatorname{res}^L_{K(\mathfrak{R}_f)}$ and $\operatorname{res}^L_{K(\mathfrak{R}_h)}$. Let $\sigma_L = (\sigma_f, \operatorname{Id}_h) \in \operatorname{Gal}(f/K) \times \operatorname{Gal}(h/K) = \operatorname{Gal}(L/K)$, where Id_h is the identity element of $\operatorname{Gal}(h/K)$ and $\sigma_f \in \operatorname{Gal}(f/K)$ is a nonidentity element, and pick any $\sigma \in \operatorname{res}_L^{-1}(\sigma_L)$. Then

$$\overline{\rho}_{2,X}(\sigma) = \alpha_X(\operatorname{res}^L_{K(\mathfrak{R}_f)}(\sigma_L)) = \alpha_X(\sigma_f) \neq \operatorname{Id}_{X_2},$$

while

$$\overline{\rho}_{2,Y}(\sigma) = \alpha_Y(\operatorname{res}^L_{K(\mathfrak{R}_h)}(\sigma_L)) = \alpha_Y(\operatorname{Id}_h) = \operatorname{Id}_{Y_2} .$$

Therefore, the $\operatorname{Gal}(K)$-modules X_2 and Y_2 are not isomorphic.

□

6. The centralizer of endomorphisms defined over base field.

This section contains preliminary investigations required for the proof of Theorem 7.1 about the impossibility of the supersingular outcome in characteristics $p > 2$ when p splits in the quadratic field $D = \mathbb{Q}(\omega) \cong \operatorname{End}^0_K(X)$. First, we

determine the algebraic structure and places of ramification of the centralizer of $i(D) = \mathrm{End}^0_K(X)$ in $\mathrm{End}^0(X)$ in the case when X is supersingular. Put

$$\begin{aligned}\mathrm{End}^0(X,i) &= \{u \in \mathrm{End}^0(X) \mid i(y)u = ui(y) \quad \forall y \in D\}\\ &= \{u \in \mathrm{End}^0(X) \mid i(\omega)u = ui(\omega)\}.\end{aligned}$$

It is well-known that when X is a supersingular abelian surface, then $\mathrm{End}^0(X) \cong \mathrm{Mat}_2(\mathbb{H}_p)$, where $\mathbb{H}_p$ a quaternion $\mathbb{Q}$-algebra ramified exactly at p and ∞. We write $\mathbb{H}_{p,D}$ for $\mathbb{H}_p \otimes_{\mathbb{Q}} D$. Both $\mathrm{End}^0(X,i)$ and $\mathbb{H}_{p,D}$ carry natural structures of D-algebras.

Theorem 6.1. *The D-algebras $\mathrm{End}^0(X,i)$ and $\mathbb{H}_{p,D}$ are isomorphic.*

Proof. We begin by showing that the isomorphism class of the D-algebra $\mathrm{End}^0(X,i)$ is independent of the embedding of D into $\mathrm{End}^0(X)$ that sends 1 to the identity automorphism of X. Let $j : D \hookrightarrow \mathrm{End}^0(X)$ be another such embedding. The $\mathbb{Q}$-algebra $i(D)$ is a simple $\mathbb{Q}$-subalgebra of the simple central $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$ and $ji^{-1} : i(D) \to j(D)$ is an algebra isomorphism. By Skolem-Noether theorem [3, p. 69], there exists $\sigma \in \mathrm{Aut}(\mathrm{End}^0(X))$ such that $ji^{-1}(x) = \sigma(x)$ for all $x \in i(D)$. Then σ is a $\mathbb{Q}$-algebra isomorphism between $\mathrm{End}^0(X,i)$ and $\mathrm{End}^0(X,j)$. Indeed, for every $z \in \mathrm{End}^0(X,i)$, we have

$$i(\omega)^{-1} z i(\omega) = z$$

and so

$$\sigma(i(\omega))^{-1}\sigma(z)\sigma(i(\omega)) = \sigma(z).$$

Taking into account that $\sigma(i(\omega)) = j(\omega)$, we obtain

$$j(\omega)^{-1}\sigma(z)j(\omega) = \sigma(z),$$

that is, $\sigma(z) \in \mathrm{End}^0(X,j)$. The map $\sigma : \mathrm{End}^0(X,i) \to \mathrm{End}^0(X,j)$ is obviously invertible.

Fix an isomorphism $\mathrm{End}^0(X) \cong \mathrm{Mat}_2(\mathbb{H}_p)$ and let $j : D \hookrightarrow \mathrm{End}^0(X)$ be given by

$$1 \mapsto \mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \omega \mapsto \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}.$$

Assume $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{H}_p)$ commutes with $j(\omega)$. Then $r = u$ and $s = td$,

$$M = \begin{pmatrix} r & td \\ t & r \end{pmatrix} = r\,\mathrm{Id} + tj(\omega),$$

and the centralizer of $j(D)$ in $\mathrm{End}^0(X)$ is generated over $\mathbb{H}_p$ by Id and $j(\omega)$. Therefore $\mathrm{End}^0(X,j)$ ($\cong \mathrm{End}^0(X,i)$) is isomorphic to $\mathbb{H}_p + j(\omega)\mathbb{H}_p = j(D)\mathbb{H}_p$, the subalgebra generated by the products of elements in $j(D)$ and $\mathbb{H}_p$.

Let $\mathbb{H}_p \otimes_{\mathbb{Q}} D \to D\mathbb{H}_p$ be the $\mathbb{Q}$-algebra homomorphism induced by $a \otimes b \mapsto ab$. Since $\mathbb{H}_p \otimes_{\mathbb{Q}} D$ is a simple algebra, the kernel of this map is either trivial or is the entire $\mathbb{H}_p \otimes_{\mathbb{Q}} D$. Because this homomorphism is not zero, it must be an embedding. A comparison of dimensions over $\mathbb{Q}$ yields $\mathrm{End}^0(X,i) \cong D\mathbb{H}_p \cong \mathbb{H}_p \otimes_{\mathbb{Q}} D$. □

It is well-known [22, p. 4] that $\mathbb{H}_p \otimes_{\mathbb{Q}} D$ is a quaternion algebra over D.

Lemma 6.2. *Let π be a place of D dividing p. The quaternion algebra $\mathrm{End}^0(X,i)$ ramifies at π if and only if p splits in D,*

Proof. For a prime $\pi|p$ of D, the degree $[D_\pi : \mathbb{Q}_p]$ equals to the product $e_\pi f_\pi$ of ramification index and relative degree of π over p. This product equals 1 if p splits in D and 2 otherwise. *Cancellation of ramification* at p occurs if and only if the degree of this extension is even (see [22, Ch. II, Th. 1.3, p. 33]). □

In Section 7 we will demonstrate that if X is a supersingular abelian variety, then $\mathrm{End}^0(X, i)$ is isomorphic to a direct summand of the group algebra $D[\mathrm{SL}_2(\mathbb{F}_5)]$. The following lemma will be used in the proof of Theorem 7.2:

Lemma 6.3. *Let* $\Gamma = \mathrm{SL}_2(\mathbb{F}_5)$*, let* D *be a real quadratic field, and* p *a prime such that* $\mathbb{H}_{p,D} = \mathbb{H}_p \otimes_{\mathbb{Q}} D$ *is a quaternion* D*-algebra. Suppose that the group algebra* $D[\Gamma]$ *contains a direct summand isomorphic to* $\mathbb{H}_{p,D}$*. Then the rational prime* p *does not split in* D*.*

Proof. Since
$$\mathrm{End}^0(X, i) \otimes_D \mathbb{C} \cong \mathrm{Mat}_2(\mathbb{C}),$$
the simple algebra $\mathbb{H}_{p,D}$ corresponds to a faithful irreducible character χ of Γ over D of degree 2.

In the notation of [5, Table II], $\chi = \zeta_i$, $i = 1$ or 2. Over $\mathbb{Q}$ we have $m_\ell(\chi) = m_{\mathbb{Q}_\ell}(\chi) = 1$ for all places ℓ of $\mathbb{Q}$ except for ∞. This result can be extended to primes of D by means of Theorem 2.16 in [5], which says that for extension D_λ of $\mathbb{Q}_\ell$, where λ is a prime of D diviging ℓ, we have
$$m_\lambda(\chi) = \frac{m_\ell(\chi)}{(m_\ell(\chi), [D_\lambda(\chi) : \mathbb{Q}_\ell(\chi)])}.$$
Therefore,
$$m_\lambda(\chi) = m_{D_\lambda}(\chi) = 1.$$
for $\lambda|\ell$. This means that $\mathbb{H}_{p,D}$ does not ramify at any non-archimedean place of D, and, by Lemma 6.2, p does not split in D. □

7. Non-Supersingularity

In this section we prove the following theorem.

Theorem 7.1. *Assume the conditions of Theorem 1.1 hold for a quadratic field* D *of reduced discriminant* d*, polynomial* f*, and abelian variety* $X = J(C_f)$*. In addition, assume that* $p = \mathrm{char}(K) > 2$ *splits in* D*. Then* X *is not a supersingular abelian variety.*

Recall that if ℓ is an odd prime, then $\ell|d$ means that ℓ ramifies in D, $(d/\ell) = -1$ means that ℓ is inert in D, and $(d/\ell) = 1$ means that ℓ splits in D. Since $d \equiv 5 \pmod 8$, the rational prime 2 is inert in D, and $D_2 := D \otimes_{\mathbb{Q}} \mathbb{Q}_2$ is a field.

The proof of Theorem 7.1 will require the following proposition, whose proof will be given later in this section.

Theorem 7.2. *Let* F *be a field of characteristic* $p > 2$ *containing all 2-power roots of unity. Let* $G = \mathrm{PSL}_2(\mathbb{F}_5)$ *and* D *be a real quadratic field with* $\delta(D) \equiv 5 \bmod 8$*. Suppose* X *is an abelian variety defined over* F*, and assume that the following conditions hold:*

(a) X *is supersingular and* $\dim(X) = 2$*;*
(b) *there exists an injective* $\mathbb{Q}$*-algebra homomorphism* $i : D \hookrightarrow \mathrm{End}^0_F(X)$ *such that* $i(1) = \mathrm{Id}_X$*, the identity automorphism of* X*;*

(c) *the image of* $\mathrm{Gal}(F)$ *in* $\mathrm{Aut}(X_2)$ *is isomorphic to* G *and the corresponding faithful representation*

$$\overline{\rho} : G \hookrightarrow \mathrm{Aut}(X_2) \cong \mathrm{GL}_4(\mathbb{F}_2)$$

satisfies

$$\mathrm{End}_G(X_2) = \mathbb{F}_4.$$

Then there exists a surjective group homomoprhism

$$\pi_1 : G_1 \twoheadrightarrow G$$

enjoying the following properties:

(i) $G_1 \cong \mathrm{SL}_2(\mathbb{F}_5)$.

(ii) *One may lift* $\overline{\rho}\pi_1 : G_1 \to \mathrm{Aut}(X_2)$ *to a faithful absolutely irreducible over the field* $D_2 = D \otimes_{\mathbb{Q}} \mathbb{Q}_2$ *symplectic representation*

$$\rho : G_1 \hookrightarrow \mathrm{Aut}_{D_2}(V_2(X))$$

in such a way that the following conditions hold:

- $\rho(G_1) \subset \mathrm{End}^0(X,i)^\times$, *where* $\mathrm{End}^0(X,i)$ *is the centralizer of* $i(D)$ *in* $\mathrm{End}^0(X)$.
- *The homomorphism from the group algebra* $D[G_1]$ *to* $\mathrm{End}^0(X,i)$ *induced by* ρ *is surjective and identifies* $\mathrm{End}^0(X,i)$ *with a direct summand of* $D[G_1]$.

Proof of Theorem 7.1. Assume that $X = J(C_f)$ satisfies conditions of Theorem 1.1 and is a supersingular abelian variety.

Let $F \subset K_a$ be a field obtained from K by adjoining all 2-power roots of unity. Then

$$D \hookrightarrow \mathrm{End}^0_K(X) \subset \mathrm{End}^0_F(X).$$

Moverover, the polynomial f remains irreducible over F and the Galois group of its splitting field over F is still $\mathbb{A}_5$, a perfect group. Indeed, F is an abelian extension of K and $\mathrm{Gal}(F/K)$ does not contain $\mathbb{A}_5$. Thus f and X satisfy the conditions of Theorem 1.1 over F. From Theorem 7.2 and Lemma 6.3 it follows that p does not split in D. $\square$

Proof of Theorem 7.2. This proof is a modification of the proof of Theorem 3.3 in [30], and most of what follows is actually stated in that work.

Let $T_2(X)$ denote the $\mathbb{Z}_2$-adic Tate module of X, $V_2(X) := T_2(X) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$ the $\mathbb{Q}_2$-adic Tate module of X, and let

$$\rho_{2,X} : \mathrm{Gal}(F) \to \mathrm{Aut}_{\mathbb{Z}_2}(T_2(X))$$

be the corresponding 2-adic representation. Put

$$H := \rho_{2,X}(\mathrm{Gal}(F)) \subset \mathrm{Aut}_{\mathbb{Z}_2}(T_2(X)).$$

Claim 1. *The group* H *is finite.*

Proof of Claim 1. The rank of the $\mathbb{Z}_2$-module $T_2(X)$ is $2\dim(X) = 4$, and, as Galois module,

$$X_2 = T_2(X)/2T_2(X).$$

If we compose $\rho_{2,X}$ with the surjective reduction modulo 2 map

$$\mathrm{Aut}_{\mathbb{Z}_2}(T_2(X)) \to \mathrm{Aut}(X_2),$$

we get a natural homomorphism

$$\overline{\rho}_{2,X} : \mathrm{Gal}(F) \to \mathrm{Aut}(X_2),$$

which defines the action of $\mathrm{Gal}(F)$ on points of X_2. Restriction of $\overline{\rho}_{2,X}$ to H yields a natural continuous surjection

$$\pi : H \to \overline{\rho}_{2,X}(\mathrm{Gal}(F)) \cong G \subset \mathrm{Aut}(X_2).$$

The choice of polarization on X gives a non-degenerate alternating bilinear form (Riemann form)

$$e : V_2(X) \times V_2(X) \to \mathbb{Q}_2.$$

Since F contains all 2-power roots of unity, e is $\mathrm{Gal}(F)$-invariant and hence H-invariant. Thus

$$H \subset \mathrm{Sp}(V_2(X), e)$$

and the H-module $V_2(X)$ is symplectic.

There exists a finite Galois extension L of F over which all endomorphisms of X are defined, that is,

$$\mathrm{End}_L(X) = \mathrm{End}(X).$$

Then then group $\mathrm{Gal}(L)$ is an open subgroup of finite index in $\mathrm{Gal}(F)$, and the group

$$H' := \rho_{2,X}(\mathrm{Gal}(L))$$

is an open normal subgroup of finite index in H.

There exists a natural embedding

$$\mathrm{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_2 \hookrightarrow \mathrm{End}_{\mathbb{Q}_2}(V_2(X)),$$

and, since X is supersingular,

$$\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) = (2\dim(X))^2 = \dim_{\mathbb{Q}_2}(\mathrm{End}_{\mathbb{Q}_2}(V_2(X))),$$

which implies that

$$\mathrm{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_2 = \mathrm{End}_{\mathbb{Q}_2}(V_2(X)).$$

Since all endomorphisms of X are defined over L, the image $\rho_{2,X}(\mathrm{Gal}(L))$ in $\mathrm{Aut}_{\mathbb{Q}_2}(V_2(X))$ commutes with $\mathrm{End}^0(X)$, and therefore with the whole

$$\mathrm{End}_{\mathbb{Q}_2}(V_2(X)) = \mathrm{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_2.$$

This implies that

$$H' = \rho_{2,X}(\mathrm{Gal}(L)) \subset \mathbb{Q}_2 \cdot \mathrm{Id}_{V_2(X)}.$$

Since

$$H' = \rho_{2,X}(\mathrm{Gal}(L)) \subset \rho_{2,X}(\mathrm{Gal}(F)) \subset \mathrm{Sp}(V_2(X), e) \subset \mathrm{SL}(V_2(X)),$$

we have

$$H' \subset \mathrm{SL}(V_2(X)) \cap \mathbb{Q}_2 \cdot \mathrm{Id}_{V_2(X)},$$

and the group $H' = \rho_{2,X}(\mathrm{Gal}(L))$ is finite. As it is a subgroup of finite index in $H = \rho_{2,X}(\mathrm{Gal}(F))$, the group H is also finite. $\square$

Since H is finite, there exists a minimal subgroup G_1 of H such that $\pi(G_1) = G$. Denote the restriction of $\pi : H \to G$ to G_1 by $\pi_1 : G_1 \twoheadrightarrow G$. Put

$$E := \mathrm{End}_{G_1}(V_2(X)) \subset \mathrm{End}_{\mathbb{Q}_2}(V_2(X)). \tag{7.1}$$

Claim 2. *The algebra E is a quadratic field extension of $\mathbb{Q}_2$ and*

$$E \cong D \otimes_{\mathbb{Q}} \mathbb{Q}_2.$$

Proof of Claim 2. The $\mathbb{Z}_2$-algebra

$$\mathcal{O} = E \cap \mathrm{End}_{\mathbb{Z}_2}(T_2(X))$$

is a free $\mathbb{Z}_2$-module, whose $\mathbb{Z}_2$-rank coincides with $\dim_{\mathbb{Q}_2}(E)$. The map

$$\mathcal{O}/2\mathcal{O} \to \mathrm{End}_{\mathbb{Z}_2}(T_2(X))/2\,\mathrm{End}_{\mathbb{Z}_2}(T_2(X)) = \mathrm{End}(X_2)$$

is an embedding. The $\mathbb{Z}_2$-rank of $\mathcal{O}$ equals the $\mathbb{F}_2$-dimension of the image of $\mathcal{O}/2\mathcal{O}$ in $\mathrm{End}_G(X_2)$. Since elements of $\mathcal{O}$ commute with G_1 in $\mathrm{End}_{\mathbb{Z}_2}(T_2(X))$, the image of $\mathcal{O}/2\mathcal{O}$ lies in $\mathrm{End}_G(X_2) \cong \mathbb{F}_4$. This implies

$$\dim_{\mathbb{Q}_2}(E) = \mathrm{rank}_{\mathbb{Z}_2} \mathcal{O} = \dim_{\mathbb{F}_2}(\mathcal{O}/2\mathcal{O}) \leq 2.$$

Let $F_1 \subset F_a$ be the subfield fixed elementwise by

$$\{\sigma \in \mathrm{Gal}(F) \mid \rho_{2,X}(\sigma) \in G_1\}$$

Then F_1 is a finite separable extension of F and

$$G_1 = \rho_{2,X}(\mathrm{Gal}(F_1)).$$

The image $\overline{\rho}_{2,X}(\mathrm{Gal}(F_1))$ in $\mathrm{Aut}(X_2)$ coincides with G.

Since $F \subset F_1$, we have $i(D) \subset \mathrm{End}^0_F(X) \subset \mathrm{End}^0_{F_1}(X)$ and so

$$\begin{aligned} i(D) \otimes_{\mathbb{Q}} \mathbb{Q}_2 &\subset \mathrm{End}^0_{F_1}(X) \otimes_{\mathbb{Q}} \mathbb{Q}_2 \\ &\subset \mathrm{End}_{\mathrm{Gal}(F_1)}(V_2(X)) \\ &= \mathrm{End}_{G_1}(V_2(X)) \\ &= E. \end{aligned}$$

Therefore

$$\dim_{\mathbb{Q}_2}(i(D) \otimes_{\mathbb{Q}} \mathbb{Q}_2) = 2 \leq \dim_{\mathbb{Q}_2}(E) \leq 2,$$

so $\dim_{\mathbb{Q}_2}(E) = 2$ and $E = i(D) \otimes_{\mathbb{Q}} \mathbb{Q}_2$. We also get

$$\mathrm{End}^0_F(X) = \mathrm{End}^0_{F_1}(X) = i(D).$$

□

This provides $V_2(X)$ with a structure of a 2-dimensional E-vector space and gives us a faithful representation

$$\rho : G_1 \to \mathrm{Aut}_E(V_2(X)) \cong \mathrm{GL}_2(E),$$

which must be absolutely irreducible by choice (7.1) of E.

Claim 3. *The G_1-module $V_2(X)$ is very simple over E.*

Proof of Claim 3. Since $\pi(G_1) = G$, by [28, Remark 5.2(i)] and Corollary 4.5, the G_1-module X_2 is very simple over $\mathbb{F}_4$.

Let $\mathcal{O}_E$ be the valuation ring of the quadratic 2-adic field E, and let λ be its maximal ideal. Since the prime 2 of $\mathbb{Q}$ is inert in D, the prime ideal $\ell = 2\mathbb{Z}_2$ of $\mathbb{Z}_2$ is also inert in $\mathcal{O}_E$, the completion of the ring of integers of D with respect to the 2-adic topology. Hence $\lambda = \ell\mathcal{O}_E$. Since the degree of inertia of λ over ℓ is 2, the residue field $k(\lambda) = \mathcal{O}_E/\lambda$ is a quadratic extension of $\mathbb{Z}_2/\ell \cong \mathbb{F}_2$, that is, $k(\lambda) \cong \mathbb{F}_4$.

The abelian group $T_2(X)$ is an $\mathcal{O}_E$-lattice in $V_2(X)$, and therefore $T_2(X)/\lambda T_2(X)$ is a $k(\lambda)$-module. Since $\lambda = \ell\mathcal{O}_E$, we have

$$T_2(X)/\lambda T_2(X) = T_2(X)/(\lambda\mathcal{O}_E)T_2(X) = T_2(X)/(\ell\mathcal{O}_E)T_2(X) = X_2.$$

The $\mathcal{O}_E$-lattice $T_2(X)$ of $V_2(X)$ is G_1-stable, so the $E[G_1]$-module $V_2(X)$ is a lifting of the very simple $\mathbb{F}_4[G_1]$-module X_2. The claim follows from [28, Remark 5.2(v)]. □

Claim 4. *The group G_1 is a perfect central extension of G.*

Proof of Claim 4. Since $G \cong \mathrm{PSL}_2(\mathbb{F}_5)$ is perfect, so is G_1 (otherwise, we can replace G_1 with $[G_1, G_1]$, thus contradicting minimality of G_1).

By [28, Remark 5.2(iv)], since the G_1-module $V_2(X)$ is very simple, then either the normal subgroup $Z_1 = \ker(\pi_1 : G_1 \to G)$ of G_1 consists of scalars (that is, it lies in E), or the $E[Z_1]$-module $V_2(X)$ is absolutely simple.

We exclude the latter possibility by contradiction. The kernel Z of $\pi : H \to G$ is a subgroup of $1 + 2\,\mathrm{End}_{\mathbb{Z}_2}(T_2(X)) \cong 1 + 2\,\mathrm{Mat}_4(\mathbb{Z}_2)$. Since H is a finite group, so is Z. In addition, $(1 + 2\,\mathrm{Mat}_4(\mathbb{Z}_2))^2 \equiv 1 \pmod{2^2\,\mathrm{Mat}_4(\mathbb{Z}_2)}$. Thus, by Minkowski-Serre Lemma [19, Th. 6.3], the group Z has exponent 1 or 2.

Therefore, Z is a finite commutative group, and so is $Z_1 \subset Z$. Hence Z_1 does not admit an absolutely irreducible representation of dimension greater than 1, which contradicts $\dim_E(V_2(X)) = 2$. Thus $Z_1 = \ker \pi_1 \subset E = \mathrm{End}_{G_1}(V_2(X))$ commutes with G_1. □

Claim 5. *$G_1 \cong \mathrm{SL}_2(\mathbb{F}_5)$.*

Proof of Claim 5. It is known [6, Prop. 4.227 and Prop. 4.232(ii)] that the only perfect central extensions of $\mathrm{PSL}_2(\mathbb{F}_5)$ are $\mathrm{SL}_2(\mathbb{F}_5)$ and $\mathrm{PSL}_2(\mathbb{F}_5)$ itself. However, there are no faithful irreducible representations of $\mathrm{PSL}_2(\mathbb{F}_5)$ of dimension 2 in characteristic 0 (see [3, p. 365]). □

Claim 6. *We have $\rho(G_1) \subset \mathrm{End}^0(X, i)^\times$.*

Proof of Claim 6. We have $\overline{\rho}_{2,X}(\mathrm{Gal}(F_1)) = G$ and hence

$$\mathrm{End}_{F_1}(X) \otimes \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{End}_{\mathrm{Gal}(F_1)}(X_2) = \mathbb{F}_4$$

Let L_1 be the finite Galois extension of F_1 attached to

$$\rho_{2,X} : \mathrm{Gal}(F_1) \to \mathrm{Aut}_{\mathbb{Z}_2}(T_2(X)).$$

Then $\mathrm{Gal}(L_1/F_1) = G_1$. Since the image $\rho_{2,X}(\mathrm{Gal}(L_1))$ in $\mathrm{Aut}_{\mathbb{Z}_2}(T_2(X))$ is trivial and all 2-power torsion points of X are defined over L_1, all endomorphism of X are defined over L_1. Hence there is a natural homomorphism

$$\kappa : G_1 = \mathrm{Gal}(L_1/F_1) \to \mathrm{Aut}(\mathrm{End}(X))$$

such that

$$\mathrm{End}_{F_1}(X) = \{u \in \mathrm{End}(X) \mid \kappa(\sigma)u = u \quad \forall \sigma \in \mathrm{Gal}(L_1/F_1)\}$$

and

$$\sigma(ux) = (\kappa(\sigma)u)(\sigma(x)).$$

Further, we write ${}^{\kappa(\sigma)}u$ instead of $\kappa(\sigma)(u)$. Since all 2-power torsion points of X are defined over L_1,

$$\sigma(ux) = {}^{\kappa(\sigma)}u(\sigma(x)) \text{ for all } x \in T_2(X), u \in \mathrm{End}(X), \sigma \in G_1.$$

Since $\mathrm{Aut}(\mathrm{End}(X)) \subset \mathrm{Aut}(\mathrm{End}^0(X))$, we can extend κ to $\mathrm{End}^0(X)$. Then

$$\mathrm{End}^0_{F_1}(X) = \{u \in \mathrm{End}^0(X) \mid {}^{\kappa(\sigma)}u = u \quad \forall \sigma \in \mathrm{Gal}(L_1/F_1)\}$$

and

$$\sigma(ux) =^{\kappa(\sigma)} u(\sigma(x))$$

Recall that

$$\mathrm{End}^0(X) \subset \mathrm{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_2 = \mathrm{End}_{\mathbb{Q}_2}(V_2(X))$$

and

$$G_1 \subset \mathrm{GL}(V_2(X)) = \mathrm{End}_{\mathbb{Q}_2}(V_2(X))^{\times}.$$

It follows that

$$\sigma u \sigma^{-1} =^{\kappa(\sigma)} u.$$

By Skolem-Noether theorem, every automorphism of the central simple $\mathbb{Q}$-algebra $\mathrm{End}^0(X) \cong \mathrm{Mat}_2(\mathbb{H}_p)$ is an inner one. This implies that for each $\sigma \in G_1$ there exists $w_\sigma \in \mathrm{End}^0(X)^{\times}$ such that

$$\sigma u \sigma^{-1} = w_\sigma u w_\sigma^{-1}$$

Since the center of $\mathrm{End}^0(X)$ is $\mathbb{Q}$, the choice of w_σ is unique up to multiplication by a non-zero rational number. This implies that $w_\sigma w_\tau$ equals $w_{\sigma\tau}$ times a non-zero rational number.

Let

$$c'_\sigma = \sigma w_\sigma^{-1}.$$

Each c'_σ commutes with $\mathrm{End}^0(X)$ and hence with $\mathrm{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_2 = \mathrm{End}_{\mathbb{Q}_2}(V_2(X))$. This means that $c'_\sigma \in \mathbb{Q}_2^{\times} \, \mathrm{Id}_{V_2(X)}$. The image

$$c_\sigma \in \mathbb{Q}_2^{\times} \, \mathrm{Id}_{V_2(X)} / \mathbb{Q}^{\times} \, \mathrm{Id}_{V_2(X)} \cong \mathbb{Q}_2^{\times} / \mathbb{Q}^{\times}$$

of c'_σ in $\mathbb{Q}_2^{\times}/\mathbb{Q}^{\times}$ does not depend on the choice of w_σ. Also, the map

$$G_1 \to \mathbb{Q}_2^{\times}/\mathbb{Q}^{\times}, \sigma \mapsto c_\sigma$$

is a group homomorphism. It has to be trivial, since G_1 is perfect. Therefore,

$$c_\sigma \in \mathbb{Q}^{\times} \, \mathrm{Id}_{V_2(X)} \ \text{ for all } \sigma \in G_1.$$

and

$$\sigma = (c')^{-1} w_\sigma \in \mathrm{End}^0(X)^{\times}$$

Finally, recall that $\mathrm{End}^0_{F_1}(X) = i(D)$, so

$$i(D) = \{u \in \mathrm{End}^0(X) \mid {}^{\kappa(\sigma)}u = u \quad \forall \sigma \in \mathrm{Gal}(L_1/F_1)\},$$

and each $\sigma \in G_1 = \mathrm{Gal}(L_1/F_1)$ commutes with $i(D)$. $\square$

By combining $\rho : G_1 \hookrightarrow \mathrm{End}^0(X,i)$ and $i : D \hookrightarrow \mathrm{End}^0(X,i)$ we obtain a natural homomorphism $D[G_1] \to \mathrm{End}^0(X,i)$.

Claim 7. *The D-algebra homomorphism $D[G_1] \to \mathrm{End}^0(X,i)$ is surjective.*

Proof of Claim 7. Let M be the image of $D[G_1]$ in $\mathrm{End}^0(X,i)$ under the above map. Then $M \otimes_D E$ coincides with the image of $E[G_1] = D[G_1] \otimes_D E$ in $\mathrm{End}^0(X,i) \otimes_D E = \mathrm{End}_E(V_2(X))$. Since $E[G_1]$-module $V_2(X)$ is absolutely simple,

$$E[G_1] \to \mathrm{End}_E(V_2(X))$$

is surjective. Therefore,

$$\dim_D(M) = \dim_D(\mathrm{End}^0(X,i))$$

and $M = \mathrm{End}^0(X,i)$, which proves the claim. $\square$

Claim 8. *The D-algebra* $\mathrm{End}^0(X,i)$ *can be identified with a direct summand of* $D[G_1]$.

Proof of Claim 8. The semisimplicity of $D[G_1]$ (by Maschke's Theorem) and simplicity of $\mathrm{End}^0(X,i)$ allow us to make such an identification. □

This concludes the proof of Theorem 7.2. □

8. Examples in characteristic zero

In this section we produce examples of hyperelliptic curves defined over $\mathbb{Q}$ with real quadratic fields $\mathbb{Q}(\sqrt{5})$ as endomorphism algebras of their jacobians. For clarity, we use capital Latin letters B, C, D, T for indeterminates over a field K and lower-case letters b, c, d, t for their specializations in K. Further, we put $\eta = (\sqrt{5}-1)/2$, so that $\mathbb{Z}[\eta]$ is the ring of integers of $\mathbb{Q}(\sqrt{5})$.

The following corollary of Theorem 1.1 will be used to obtain these examples.

Corollary 8.1. *Let K be a field of characteristic 0 and $f_T(x) \in K(T)[x]$ be an irreducible separable polynomial of degree $n = 6$ in x parametrized by a variable T transcendental over K. Define a hyperelliptic curve C_T over $K(T)$ by*

$$C_T = C_{f_T} : y^2 = f_T(x).$$

Let $J(C_T)$ be its jacobian and $\mathrm{End}_{K(T)}(J(C_T))$ be the ring of $K(T)$-endomorphisms of $J(C_T)$. Assume that

(i) $\mathrm{Gal}(f_T/K(T)) \cong \mathbb{A}_5$,
(ii) $\mathrm{End}^0_{K(T)}(J(C_T))$ *is isomorphic to a real quadratic field D, and*
(iii) *for some value $t \in K$ of T the polynomial f_t is irreducible over K and* $\mathrm{Gal}(f_t/K) \cong \mathbb{A}_5$.

Then $\mathrm{End}(J(C_t))$ *is isomorphic to an order of D with*

$$\delta(\mathrm{End}(J(C_t))) \equiv 5 \bmod 8.$$

Proof. Assume that all of the conditions of Corollary 8.1 are satisfied for specialization of T to $t \in K$. The action of $\mathrm{Gal}(f_T/K(T))$ on $\mathfrak{R}_T$ extends to an action of $\mathrm{Gal}(f_T/K(T))$ on $\mathfrak{R}_t$. The action can be factored through $\mathrm{Gal}(f_t/K)$; and since $\mathrm{Gal}(f_T/K(T)) \cong \mathrm{Gal}(f_t/K)$, the $\mathrm{Gal}(f_T/K(T))$-sets $\mathfrak{R}_T$ and $\mathfrak{R}_t$ are also isomorphic. We also have $\mathrm{End}_{K(T)}(J(C_T)) \subset \mathrm{End}_K(J(C_t))$. The conclusion of the corollary follows from Theorem 1.1. □

In [7], K. Hashimoto gives the following form of Brumer's 3-parameter family of curves:

$$\begin{aligned} C_{B,C,D} : y^2 = f_{B,C,D}(x) = x^6 &+ 2Cx^5 + (2+2C+C^2-4BD)x^4 \\ &+ (2+4B+2C+2C^2-4D-8BD)x^3 \\ &+ (5+12B+4C+C^2-4BD)x^2 \\ &+ (6+12B+2C)x+4B+1. \end{aligned} \tag{8.1}$$

For indeterminates B, C, D over $\mathbb{Q}$, the algebra of endomorphisms of its jacobian $J(C_{B,C,D})$ is isomorphic to $\mathbb{Q}(\sqrt{5})$ and its endomorphisms ring $\mathrm{End}(J(C_{B,C,D})) \cong \mathbb{Z}[\eta]$. Moreover, the polynomial $f_{B,C,D}$ is irreducible over $\mathbb{Q}(B,C,D)$, and its splitting field over $\mathbb{Q}(B,C,D)$ has $\mathbb{A}_5$ as its Galois group.

Assume that for certain values of B, C, D, say $b, c, d \in \mathbb{Q}$, respectively, the polynomial $f_{b,c,d}$ is irreducible over $\mathbb{Q}$, and the Galois group of its splitting field over $\mathbb{Q}$

is isomorphic to $\mathbb{A}_5$. Then $f_{B,c,d}, f_{B,C,d}$ are also irreducible over $\mathbb{Q}(B)$ and $\mathbb{Q}(B,C)$, respectively, because their factorization would lead to a factorization of $f_{b,c,d}$ over $\mathbb{Q}$. We have a tower of groups

$$\begin{array}{rcl} \mathbb{A}_5 & \cong & \mathrm{Gal}(f_{b,c,d}/\mathbb{Q}) \\ & \subset & \mathrm{Gal}(f_{B,c,d}/\mathbb{Q}(B)) \\ & \subset & \mathrm{Gal}(f_{B,C,d}/\mathbb{Q}(B,C)) \\ & \subset & \mathrm{Gal}(f_{B,C,D}/\mathbb{Q}(B,C,D)) \\ & \cong & \mathbb{A}_5, \end{array}$$

which forces every intermediate Galois group to be isomorphic to $\mathbb{A}_5$. By applying Corollary 8.1 to the consecutive specializations we conclude that every one of them has the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{5})$ for the endomorphism ring.

By picking appropriate values b, c, d we can give examples to Corollary 8.1. As an example, we work through one of the curves given in the table. The others can be treated in a similar manner.

Example 8.2. For $b = 0$, $c = 1$, $d = 2$ we get a hyperelliptic curve

$$\begin{array}{rcl} C : y^2 & = & f_{0,1,2}(x) \\ & = & x^6 + 2x^5 + 5x^4 - 2x^3 + 10x^2 + 8x + 1 \end{array}$$

The splitting field of f is an $\mathbb{A}_5$-extension of $\mathbb{Q}$ with discriminant $1125721 = 1061^2$. By the above argument, we have $\mathrm{End}(J(C)) \cong \mathbb{Z}[\eta]$. By allowing one of the above variables to vary, say $d = T$, while fixing the other two, we can get a hyperelliptic curve

$$\begin{array}{rcl} C' : y^2 & = & f_{0,1,T}(x) \\ & = & x^6 + 2x^5 + 5x^4 + (6 - 4T)x^3 + 10x^2 + 8x + 1 \end{array}$$

defined over $\mathbb{Q}(T)$ such that $\mathrm{Gal}(f_T/\mathbb{Q}(T)) \cong \mathbb{A}_5$ by the above argument. The endomorphism ring of its jacobian is also isomorphic to $\mathbb{Z}[\eta]$.

Non-isogenuity of the jacobians of curves listed in Table 8.1 can be deduced from pairwise coprimality of the discriminants of the splitting fields of polynomials that define them.

Theorem 8.3. *If polynomials $f(x), h(x) \in \mathbb{Q}[x]$ satisfy all of the conditions of Theorem 1.1, and if the discriminants of the splitting fields of f and h over $\mathbb{Q}$ are relatively prime, then the jacobians $J(C_f)$ and $J(C_h)$ of the curves $C_f : y^2 = f(x)$ and $C_h : y^2 = h(x)$ are not isogenous.*

Proof. It is known that if L/K is an extension of algebraic number fields, then $\delta(K) | \delta(L)$ by the Discriminant Tower Theorem. This implies that the splitting fields $\mathbb{Q}(\mathfrak{R}_f)$ and $\mathbb{Q}(\mathfrak{R}_h)$ of given polynomials are linearly disjoint. Indeed, if the two fields have a common subfield, say E, then $\delta(E) = 1$ and $E = \mathbb{Q}$ by the theorem of Hermite. By Theorem 1.7, $J(C_f)$ and $J(C_h)$ are not isogenous. $\square$

By Hilbert's irreducibility theorem, there are infinitely many rational t such that $\mathrm{Gal}(f_t/\mathbb{Q}) \cong \mathbb{A}_5$. Moreover, infinitely many of these extensions are pairwise linearly disjoint over $\mathbb{Q}$. It follows from Theorem 1.7 that there is an infinite number of pairwise non-isogenous hyperelliptic jacobians of dimension 2 with $\mathbb{Z}[\eta]$ as their endomorphism ring.

For each of the curves in Table 8.1, the polynomial f is irreducible, and the splitting field of f over $\mathbb{Q}$ is an $\mathbb{A}_5$-extension. Note that the specialization $b = 1$, $c = 1$, $d = 2$ is the original example given in Brumer's paper [2]. This table was constructed with the help of PARI-GP number-theoretic package [17] through a search for integer values $-5 \le b, c, d \le 5$. The polynomials were chosen so that the discriminants of their splitting fields are pairwise relatively prime in order to ensure that the jacobian of the corresponding hyperelliptic curves are pairwise nonisogenous.

More examples can be obtained by examination of polynomials in the table in Appendix A.3 of [24]. J. Wilson proved for every polynomial f in that table, that if we define a hyperelliptic curve $C_f : y^2 = f(x)$, then $\mathbb{Z}[\eta] \subset \mathrm{End}_{\mathbb{Q}}(J(C_f))$. Therefore, if $\mathrm{Gal}(f/\mathbb{Q}) \cong \mathbb{A}_5$, then $\mathrm{End}_{\mathbb{Q}}(J(C_f)) = \mathrm{End}(J(C_f)) = \mathbb{Z}[\eta]$. For example, if $f(x) = 3x^6 + 8x^5 + 54x^4 - 26x^3 - 173x^2 + 218x - 73$, then $\mathrm{Gal}(f/\mathbb{Q}) \cong \mathbb{A}_5$, and $\mathrm{End}(J(C_f)) = \mathbb{Z}[\eta]$. It is easily shown that this polynomial is not a specialization of the family (8.1) of Brumer's curve for any $b, c, d \in \mathbb{Q}$.

TABLE 8.1. Some curves C over $\mathbb{Q}$ with $\mathrm{End}(J(C)) = \mathbb{Z}[\eta]$

b	c	d	$C : y^2 = f_{b,c,d}(x)$	$\delta(\mathbb{Q}(\mathfrak{R}_f))$
0	0	0	$y^2 = x^6 + 2x^4 + 2x^3 + 5x^2 + 6x + 1$	$2^6 \cdot 103^2$
0	1	2	$y^2 = x^6 + 2x^5 + 5x^4 - 2x^3 + 10x^2 + 8x + 1$	1061^2
0	-1	-3	$y^2 = x^6 - 2x^5 + x^4 + 14x^3 + 2x^2 + 4x + 1$	$11^2 \cdot 137^2$
0	-1	5	$y^2 = x^6 - 2x^5 + x^4 - 18x^3 + 2x^2 + 4x + 1$	2293^2
0	3	-3	$y^2 = x^6 + 6x^5 + 17x^4 + 38x^3 + 26x^2 + 12x + 1$	4483^2
0	3	5	$y^2 = x^6 + 6x^5 + 17x^4 + 6x^3 + 26x^2 + 12x + 1$	$3^2 \cdot 4441^2$
0	-3	-2	$y^2 = x^6 - 6x^5 + 5x^4 + 22x^3 + 2x^2 + 1$	2609^2
0	4	2	$y^2 = x^6 + 8x^5 + 26x^4 + 34x^3 + 37x^2 + 14x + 1$	$53^2 \cdot 79^2$
0	4	-2	$y^2 = x^6 + 8x^5 + 26x^4 + 50x^3 + 37x^2 + 14x + 1$	2707^2
0	-4	2	$y^2 = x^6 - 8x^5 + 10x^4 + 18x^3 + 5x^2 - 2x + 1$	2029^2
0	-4	-2	$y^2 = x^6 - 8x^5 + 10x^4 + 34x^3 + 5x^2 - 2x + 1$	6827^2
0	5	2	$y^2 = x^6 + 10x^5 + 37x^4 + 54x^3 + 50x^2 + 16x + 1$	$17^2 \cdot 337^2$
0	5	-2	$y^2 = x^6 + 10x^5 + 37x^4 + 70x^3 + 50x^2 + 16x + 1$	$5^2 \cdot 757^2$
0	-5	1	$y^2 = x^6 - 10x^5 + 17x^4 + 38x^3 + 10x^2 - 4x + 1$	3929^2
0	-5	5	$y^2 = x^6 - 10x^5 + 17x^4 + 22x^3 + 10x^2 - 4x + 1$	$47^2 \cdot 251^2$
1	0	4	$y^2 = x^6 - 14x^4 - 42x^3 + x^2 + 18x + 5$	$41^2 \cdot 941^2$
1	-1	2	$y^2 = x^6 - 2x^5 - 7x^4 - 18x^3 + 6x^2 + 16x + 5$	7933^2
1	-1	-2	$y^2 = x^6 - 2x^5 + 9x^4 + 30x^3 + 22x^2 + 16x + 5$	$19^2 \cdot 1289^2$
1	2	2	$y^2 = x^6 + 4x^5 + 2x^4 - 6x^3 + 21x^2 + 22x + 5$	2861^2
1	-2	2	$y^2 = x^6 - 4x^5 - 6x^4 - 14x^3 + 5x^2 + 14x + 5$	9907^2
1	-2	-2	$y^2 = x^6 - 4x^5 + 10x^4 + 34x^3 + 21x^2 + 14x + 5$	$71^2 \cdot 607^2$
1	-3	0	$y^2 = x^6 - 6x^5 + 5x^4 + 18x^3 + 14x^2 + 12x + 5$	3089^2
1	-3	4	$y^2 = x^6 - 6x^5 - 11x^4 - 30x^3 - 2x^2 + 12x + 5$	$23^2 \cdot 3137^2$
1	4	4	$y^2 = x^6 + 8x^5 + 10x^4 - 2x^3 + 33x^2 + 26x + 5$	17509^2
1	4	-4	$y^2 = x^6 + 8x^5 + 42x^4 + 94x^3 + 65x^2 + 26x + 5$	55763^2
1	5	-4	$y^2 = x^6 + 10x^5 + 53x^4 + 114x^3 + 78x^2 + 28x + 5$	55793^2

b	c	d	$C : y^2 = f_{b,c,d}(x)$	$\delta(\mathbb{Q}(\mathfrak{R}_f))$
1	−5	2	$y^2 = x^6 - 10x^5 + 9x^4 + 22x^3 + 14x^2 + 8x + 5$	34729^2
−1	1	3	$y^2 = x^6 + 2x^5 + 17x^4 + 14x^3 + 10x^2 - 4x - 3$	11027^2
−1	1	−5	$y^2 = x^6 + 2x^5 - 15x^4 - 18x^3 - 22x^2 - 4x - 3$	17387^2
−1	−1	3	$y^2 = x^6 - 2x^5 + 13x^4 + 10x^3 + 2x^2 - 8x - 3$	9293^2
−1	−1	−5	$y^2 = x^6 - 2x^5 - 19x^4 - 22x^3 - 30x^2 - 8x - 3$	26501^2
−1	−2	3	$y^2 = x^6 - 4x^5 + 14x^4 + 14x^3 + x^2 - 10x - 3$	$13^2 \cdot 1151^2$
−1	4	3	$y^2 = x^6 + 8x^5 + 38x^4 + 50x^3 + 37x^2 + 2x - 3$	$157^2 \cdot 389^2$
−1	4	−5	$y^2 = x^6 + 8x^5 + 6x^4 + 18x^3 + 5x^2 + 2x - 3$	$43^2 \cdot 227^2$
−1	−4	3	$y^2 = x^6 - 8x^5 + 22x^4 + 34x^3 + 5x^2 - 14x - 3$	$59^2 \cdot 1483^2$
−1	−4	−5	$y^2 = x^6 - 8x^5 - 10x^4 + 2x^3 - 27x^2 - 14x - 3$	83417^2
−1	5	3	$y^2 = x^6 + 10x^5 + 49x^4 + 70x^3 + 50x^2 + 4x - 3$	$73^2 \cdot 1511^2$
−1	5	−5	$y^2 = x^6 + 10x^5 + 17x^4 + 38x^3 + 18x^2 + 4x - 3$	50423^2
2	0	−3	$y^2 = x^6 + 26x^4 + 70x^3 + 53x^2 + 30x + 9$	$167^2 \cdot 181^2$
2	−1	4	$y^2 = x^6 - 2x^5 - 31x^4 - 70x^3 - 6x^2 + 28x + 9$	$61^2 \cdot 2593^2$
2	−1	−4	$y^2 = x^6 - 2x^5 + 33x^4 + 90x^3 + 58x^2 + 28x + 9$	$457^2 \cdot 2011^2$
2	−2	4	$y^2 = x^6 - 4x^5 - 30x^4 - 66x^3 - 7x^2 + 26x + 9$	$107^2 \cdot 2693^2$
2	−2	−4	$y^2 = x^6 - 4x^5 + 34x^4 + 94x^3 + 57x^2 + 26x + 9$	1280761^2
2	4	5	$y^2 = x^6 + 8x^5 - 14x^4 - 50x^3 + 21x^2 + 38x + 9$	80407^2
2	−4	−3	$y^2 = x^6 - 8x^5 + 34x^4 + 94x^3 + 53x^2 + 22x + 9$	$673^2 \cdot 2087^2$
2	5	−3	$y^2 = x^6 + 10x^5 + 61x^4 + 130x^3 + 98x^2 + 40x + 9$	$31^4 \cdot 233^2$
2	5	5	$y^2 = x^6 + 10x^5 - 3x^4 - 30x^3 + 34x^2 + 40x + 9$	145487^2
2	−5	0	$y^2 = x^6 - 10x^5 + 17x^4 + 50x^3 + 34x^2 + 20x + 9$	29663^2
2	−5	4	$y^2 = x^6 - 10x^5 - 15x^4 - 30x^3 + 2x^2 + 20x + 9$	271273^2
−2	0	−3	$y^2 = x^6 - 22x^4 - 42x^3 - 43x^2 - 18x - 7$	32771^2
−2	−1	−4	$y^2 = x^6 - 2x^5 - 31x^4 - 54x^3 - 54x^2 - 20x - 7$	$29^2 \cdot 3319^2$
−2	−2	4	$y^2 = x^6 - 4x^5 + 34x^4 + 46x^3 + 9x^2 - 22x - 7$	11057^2
−2	3	4	$y^2 = x^6 + 6x^5 + 49x^4 + 66x^3 + 34x^2 - 12x - 7$	582983^2
−2	−3	−3	$y^2 = x^6 - 6x^5 - 19x^4 - 30x^3 - 46x^2 - 24x - 7$	72101^2
−2	4	5	$y^2 = x^6 + 8x^5 + 66x^4 + 94x^3 + 53x^2 - 10x - 7$	$7^2 \cdot 228281^2$
−2	−4	−3	$y^2 = x^6 - 8x^5 - 14x^4 - 18x^3 - 43x^2 - 26x - 7$	144223^2
−2	5	5	$y^2 = x^6 + 10x^5 + 77x^4 + 114x^3 + 66x^2 - 8x - 7$	$317^2 \cdot 7057^2$
3	0	−5	$y^2 = x^6 + 62x^4 + 154x^3 + 101x^2 + 42x + 13$	5562929^2
3	1	3	$y^2 = x^6 + 2x^5 - 31x^4 - 66x^3 + 10x^2 + 44x + 13$	$67^2 \cdot 2617^2$
3	−1	−5	$y^2 = x^6 - 2x^5 + 61x^4 + 154x^3 + 98x^2 + 40x + 13$	6683357^2
3	2	−5	$y^2 = x^6 + 4x^5 + 70x^4 + 166x^3 + 113x^2 + 46x + 13$	$223^2 \cdot 20549^2$
3	−3	3	$y^2 = x^6 - 6x^5 - 31x^4 - 58x^3 + 2x^2 + 36x + 13$	384641^2
3	−4	−5	$y^2 = x^6 - 8x^5 + 70x^4 + 178x^3 + 101x^2 + 34x + 13$	14931629^2
3	−5	−1	$y^2 = x^6 - 10x^5 + 29x^4 + 82x^3 + 58x^2 + 32x + 13$	$229^2 \cdot 2897^2$
−3	1	−4	$y^2 = x^6 + 2x^5 - 43x^4 - 86x^3 - 74x^2 - 28x - 11$	$269^2 \cdot 3109^2$
−3	−3	4	$y^2 = x^6 - 6x^5 + 53x^4 + 82x^3 + 14x^2 - 36x - 11$	$1493^2 \cdot 2161^2$
−3	−4	−4	$y^2 = x^6 - 8x^5 - 38x^4 - 66x^3 - 79x^2 - 38x - 11$	238991^2
−3	5	−4	$y^2 = x^6 + 10x^5 - 11x^4 - 30x^3 - 34x^2 - 20x - 11$	236813^2
−3	−5	2	$y^2 = x^6 - 10x^5 + 41x^4 + 70x^3 - 2x^2 - 40x - 11$	1066643^2

b	c	d	$C : y^2 = f_{b,c,d}(x)$	$\delta(\mathbb{Q}(\mathfrak{R}_f))$
4	−1	5	$y^2 = x^6 - 2x^5 - 79x^4 - 162x^3 - 30x^2 + 52x + 17$	$991^2 \cdot 5441^2$
4	−3	−2	$y^2 = x^6 - 6x^5 + 37x^4 + 102x^3 + 82x^2 + 48x + 17$	1776617^2
4	−4	2	$y^2 = x^6 - 8x^5 - 22x^4 - 30x^3 + 21x^2 + 46x + 17$	$37^2 \cdot 8161^2$
4	−4	−2	$y^2 = x^6 - 8x^5 + 42x^4 + 114x^3 + 85x^2 + 46x + 17$	$331^2 \cdot 8297^2$
4	−5	1	$y^2 = x^6 - 10x^5 + x^4 + 22x^3 + 42x^2 + 44x + 17$	123829^2
−4	−1	5	$y^2 = x^6 - 2x^5 + 81x^4 + 126x^3 + 34x^2 - 44x - 15$	$89^2 \cdot 154127^2$
−4	2	5	$y^2 = x^6 + 4x^5 + 90x^4 + 138x^3 + 49x^2 - 38x - 15$	$139^2 \cdot 94651^2$
−4	−5	−3	$y^2 = x^6 - 10x^5 - 31x^4 - 58x^3 - 86x^2 - 52x - 15$	500111^2
5	−4	0	$y^2 = x^6 - 8x^5 + 10x^4 + 46x^3 + 65x^2 + 58x + 21$	65003^2
−5	1	−5	$y^2 = x^6 + 2x^5 - 95x^4 - 194x^3 - 150x^2 - 52x - 19$	$3301^2 \cdot 5783^2$
−5	−1	−5	$y^2 = x^6 - 2x^5 - 99x^4 - 198x^3 - 158x^2 - 56x - 19$	15327437^2
−5	−4	3	$y^2 = x^6 - 8x^5 + 70x^4 + 114x^3 + 5x^2 - 62x - 19$	9647317^2

9. Examples in Positive Characteristic

Examples of hyperelliptic curves satisfying conditions of Theorem 1.1 can be found by reducing examples defined over $\mathbb{Q}(T)$ (for example, specializations of the Brumer's family) modulo odd primes. We need to make sure that after reduction the defining polynomial remains irreducible, separable, and has Galois group $\mathbb{A}_5$.

In positive characteristic it becomes necessary to distinguish between the two outcomes of that theorem. Let $\mathrm{char}(K) = p > 2$,

$$f(x) = x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

be a polynomial with distinct roots over K_a, and let $f(x)^{(p-1)/2} = \sum c_i x^i$. Then the Cartier-Manin/Hasse-Witt matrix [15, 25] for the hyperelliptic curve $C : y^2 = f(x)$ is the matrix obtained from

$$M = \begin{pmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{pmatrix}.$$

by extraction of pth roots of the entries. It is known [9], [25, Th. 2.2], [8] that the jacobian of the curve C is a supersingular abelian variety if and only if

$$MM^{(p)} = \begin{pmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{pmatrix} \cdot \begin{pmatrix} c_{p-1}^p & c_{p-2}^p \\ c_{2p-1}^p & c_{2p-2}^p \end{pmatrix} = 0.$$

It can be seen that this happens in one of the following cases:

(1) $c_{p-1} = c_{2p-1} = c_{2p-2} = 0$, or
(2) $c_{2p-1} \neq 0$,

$$c_{p-2} = -\frac{c_{p-1}^{p+1}}{c_{2p-1}^p} \quad \text{and} \quad c_{2p-2} = -\frac{c_{p-1}^p}{c_{2p-1}^{p-1}}.$$

Example 9.1. Let $p = \mathrm{char}(K) = 3$. Then $f(x)^{(p-1)/2} = f(x)$, and the curve $C : y^2 = f(x)$ is supersingular if and only if one of the following conditions holds:

(1) $a_2 = a_4 = a_5 = 0$. In this case, $a_1 \neq 0$, since polynomials $f(x) = x^6 + a_3x^3 + a_0$ are not separable in characteristic 3.
(2) $a_5 \neq 0$, $a_1 = -a_2^4/a_5^3$, and $a_4 = -a_2^3/a_5^2$.

This means C is supersingular if and only if either

$$f(x) = x^6 + a_3x^3 + a_1x + a_0, \quad a_1 \neq 0,$$

or

$$f(x) = x^6 + a_5x^5 - \frac{a_2^3}{a_5^2}x^4 + a_3x^3 + a_2x^2 - \frac{a_2^4}{a_5^3}x + a_0, \quad a_5 \neq 0.$$

Example 9.2. Let C_f be the smooth hyperelliptic curve $y^2 = f(x)$ over $\mathbb{F}_3(T)$, where $f(x)$ is one of the polynomials in Table 9.1. Then

$$\mathrm{End}(J(C_f)) = \mathrm{End}_{\mathbb{F}_3(T)}(J(C_f)) = \mathbb{Z}[\eta].$$

TABLE 9.1. Some curves C over $\mathbb{F}_3(T)$ with $\mathrm{End}(J(C)) = \mathbb{Z}[\eta]$

b	c	d	$C: y^2 = f_{b,c,d}(x)$ reduced modulo 3
0	1	T	$y^2 = x^6 + 2x^5 + 2x^4 + 2Tx^3 + x^2 + 2x + 1$
0	2	$T+2$	$y^2 = x^6 + x^5 + x^4 + 2Tx^3 + 2x^2 + x + 1$
1	1	$2T+1$	$y^2 = x^6 + 2x^5 + (T+1)x^4 + x^3 + Tx^2 + 2x + 2$
1	2	$T+1$	$y^2 = x^6 + x^5 + 2Tx^4 + (2T+1)x^2 + x + 2$
T	1	0	$y^2 = x^6 + 2x^5 + 2x^4 + Tx^3 + x^2 + 2x + T + 1$
$T+1$	0	$T+2$	$y^2 = x^6 + 2T^2x^4 + T^2x^3 + 2T^2x^2 + T + 2$
$T+1$	$2T$	$T+1$	$y^2 = x^6 + Tx^5 + (2T+1)x^4 + x^2 + Tx + T + 2$
$T+2$	2	0	$y^2 = x^6 + x^5 + x^4 + (T+1)x^3 + 2x^2 + x + T$
$T+2$	$2T+2$	$T+2$	$y^2 = x^6 + (T+1)x^5 + 2Tx^4 + x^2 + (T+1)x + T$
$2T+1$	0	$2T+2$	$y^2 = x^6 + 2T^2x^4 + T^2x^3 + 2T^2x^2 + 2T + 2$

Let us work through one of the examples. The smooth curve C defined over $\mathbb{F}_3(T)$ by

$$C : y^2 = x^6 + 2x^5 + 2x^4 + 2Tx^3 + x^2 + 2x + 1$$

is the reduction modulo 3 of the curve

$$C' = C_{0,1,T} : y^2 = x^6 + 2x^5 + 5x^4 + (6 - 4T)x^3 + 10x^2 + 8x + 1$$

defined over $\mathbb{Q}(T)$ which, according to Example 8.2, satisfies

$$\mathrm{End}(J(C')) = \mathrm{End}_{\mathbb{Q}(T)}(J(C')) \cong \mathbb{Z}[\eta].$$

Thus we have

$$\mathbb{Z}[\eta] \cong \mathrm{End}_{\mathbb{Q}(T)}(J(C')) \hookrightarrow \mathrm{End}_{\mathbb{F}_3(T)}(J(C)).$$

Using MAGMA Computational Algebra System [1, 21] we verify that the polynomial $f(x) = x^6 + 2x^5 + 2x^4 + 2Tx^3 + x^2 + 2x + 1$ is irreducible and separable over $\mathbb{F}_3(T)$ with $\mathrm{Gal}(f/\mathbb{F}_3(T)) \cong \mathbb{A}_5$. Finally, the procedure delineated above shows that $J(C)$ is not a supersingular abelian variety. Therefore, by Theorem 1.1 we have $\mathrm{End}(J(C)) \cong \mathbb{Z}[\eta]$.

Other examples from Table 9.1, as well as Tables 9.2, 9.4, and 9.5, are obtained in a similar fashion. Table 9.3 is generated analogously, with the distinction that only supersingular examples are selected.

All jacobians of smooth hyperelliptic curves over $\mathbb{F}_3(T)$ obtained by reduction of specializations of Brumer's family will be non-supersingular. To prove this, observe that the reduction of the Brumer's equation 8.1 modulo 3 yields

$$a_1 = a_5 \quad \text{and} \quad a_4 = a_2 + C = a_2 - a_1$$

This immediately rules out the first case of supersingularity outlined in Example 9.1. In the second case, $a_1 = a_5 \neq 0$ and

$$a_1 a_5^3 = -a_2^4,$$

so

$$a_1^4 = -a_2^4.$$

For $a_1, a_2 \in \mathbb{F}_3(T)$, this equation does not have a solution.

It is possible that supersingular examples exist over $\mathbb{F}_9(T)$. Indeed, $a_2 = \varepsilon a_1$, where ε is a root of $z^4+1=0$ in $\overline{\mathbb{F}}_3$. We also know that $a_4 a_5^2 = -a_2^3$, so $a_4 = -\varepsilon^3 a_1$. Finally, plug this into $a_4 = a_2 - a_1$ and divide by $a_1 \neq 0$, to get $\varepsilon^3 + \varepsilon - 1 = 0$. The simultaneous solutions of $z^4+1=0$ and $z^3+z-1=0$ are

$$\varepsilon = -1 \pm \sqrt{-1} \in \mathbb{F}_9.$$

Since $a_4 = 2 + 2C + C^2 - 4BD$, $a_5 = a_1 = 2C$, and $a_4 = (\varepsilon - 1)a_1$, we have

$$BD = C^2 + (\varepsilon+1)C - 1.$$

As a result, the equation of the curve will have the form

$$C : y^2 = f(x) = x^6 - Cx^5 + (1-\varepsilon)Cx^4 \\ + (1 + \varepsilon C + B - D)x^3 - \varepsilon C x^2 - Cx + (B+1).$$

In order to verify that $\mathrm{End}_{\mathbb{F}_9(T)}(J(C)) = \mathbb{Z}[\eta]$, one will need to check that C is a reduction of a curve satisfying the conditions of Theorem 1.1, that $f(x)$ is irreducible in $\mathbb{F}_9(T)[x]$, and that $\mathrm{Gal}(f/\mathbb{F}_9(T)) \cong \mathbb{A}_5$.

When $\mathrm{char}(K) > 3$, any irreducible polynomial $f(x)$ of degree 6 is separable, and therefore the curve $y^2 = f(x)$ defined by such a polynomial is smooth.

Example 9.3. Let C_f be the smooth hyperelliptic curve $y^2 = f(x)$ over $\mathbb{F}_5(T)$, where $f(x)$ is one of the polynomials in Table 9.2. Then

$$\mathrm{End}(J(C_f)) = \mathrm{End}_{\mathbb{F}_5(T)}(J(C_f)) = \mathbb{Z}[\eta].$$

TABLE 9.2. Some curves C over $\mathbb{F}_5(T)$ with $\mathrm{End}(J(C)) = \mathbb{Z}[\eta]$

b	c	d	$C : y^2 = f_{b,c,d}(x)$ reduced modulo 5
0	0	$T+3$	$y^2 = x^6 + 2x^4 + Tx^3 + x + 1$
0	2	T	$y^2 = x^6 + 4x^5 + (T+4)x^3 + 2x^2 + 1$
0	3	$T+4$	$y^2 = x^6 + x^5 + 2x^4 + Tx^3 + x^2 + 2x + 1$
0	4	$T+3$	$y^2 = x^6 + 3x^5 + x^4 + Tx^3 + 2x^2 + 4x + 1$
3	3	$2T+1$	$y^2 = x^6 + x^5 + Tx^4 + 4Tx^3 + Tx^2 + 3x + 3$
4	0	$4T+3$	$y^2 = x^6 + (T+4)x^4 + Tx^3 + Tx^2 + 4x + 2$
4	2	$4T$	$y^2 = x^6 + 4x^5 + Tx^4 + Tx^3 + Tx^2 + 3x + 2$
4	3	$4T+2$	$y^2 = x^6 + x^5 + Tx^4 + Tx^3 + (T+2)x^2 + 2$
$T+2$	$4T$	$4T+4$	$y^2 = x^6 + 3Tx^5 + 2x^2 + 4T + 4$
$T+3$	4	3	$y^2 = x^6 + 3x^5 + 3Tx^4 + 2x^2 + 2Tx + 4T + 3$
$2T+2$	$3T$	$3T+4$	$y^2 = x^6 + Tx^5 + 2x^2 + 3T + 4$
$3T+1$	$2T+4$	$2T+1$	$y^2 = x^6 + (4T+3)x^5 + 2x^4 + 4x^3 + x + 2T$
$3T+2$	0	3	$y^2 = x^6 + (4T+3)x^4 + Tx + 2T + 4$
$3T+2$	$2T$	$2T+4$	$y^2 = x^6 + 4Tx^5 + 2x^2 + 2T + 4$
$3T+3$	$2T+2$	$2T+4$	$y^2 = x^6 + (4T+4)x^5 + 2x^4 + 4x^3 + x + 2T + 3$

b	c	d	$C : y^2 = f_{b,c,d}(x)$ reduced modulo 5
$3T+4$	$2T+1$	$2T+3$	$y^2 = x^6 + (4T+2)x^5 + 2x^4 + 4x^3 + x + 2T + 2$
$3T+4$	$2T+3$	$2T+2$	$y^2 = x^6 + (4T+1)x^5 + 2x^2 + 2T + 2$
$4T+1$	1	3	$y^2 = x^6 + 2x^5 + (2T+3)x^4 + 4x^3 + 3Tx + T$
$4T+1$	$T+4$	$T+1$	$y^2 = x^6 + (2T+3)x^5 + 2x^4 + 4x^3 + x + T$
$4T+1$	$2T$	$4T+3$	$y^2 = x^6 + 4Tx^5 + Tx^3 + 2Tx^2 + (2T+3)x + T$
$4T+2$	T	$T+4$	$y^2 = x^6 + 2Tx^5 + 2x^2 + T + 4$
$4T+3$	$T+2$	$T+4$	$y^2 = x^6 + (2T+4)x^5 + 2x^4 + 4x^3 + x + T + 3$

Example 9.4. Let C_f be the smooth hyperelliptic curve $y^2 = f(x)$ over $\mathbb{F}_5(T)$, where $f(x)$ is one of the polynomials in Table 9.3. Then

$$\mathrm{End}_{\mathbb{F}_5(T)}(J(C_f)) = \mathbb{Z}[\eta].$$

but $J(C)$ is a supersingular abelian variety; that is, $\mathrm{End}^0(J(C_f)) = \mathrm{Mat}_2(\mathbb{H}_5)$.

TABLE 9.3. Some supersingular curves C over $\mathbb{F}_5(T)$ with $\mathrm{End}_{\mathbb{F}_5(T)}(J(C)) = \mathbb{Z}[\eta]$

b	c	d	$C : y^2 = f_{b,c,d}(x)$ reduced modulo 5
0	1	T	$y^2 = x^6 + 2x^5 + (T+1)x^3 + 3x + 1$
T	$4T+3$	$4T+3$	$y^2 = x^6 + (3T+1)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 4T + 1$
$T+1$	$4T+2$	$4T+2$	$y^2 = x^6 + (3T+4)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 4T$
$T+2$	$4T+1$	$4T+1$	$y^2 = x^6 + (3T+2)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 4T + 4$
$T+1$	$4T+2$	$4T+2$	$y^2 = x^6 + (3T+4)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 4T$
$T+2$	$4T+1$	$4T+1$	$y^2 = x^6 + (3T+2)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 4T + 4$
$T+3$	$4T$	$4T$	$y^2 = x^6 + 3Tx^5 + 2x^4 + 4x^3 + x^2 + 2x + 4T + 3$
$T+4$	$4T+4$	$4T+4$	$y^2 = x^6 + (3T+3)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 4T + 2$
$2T$	$3T+3$	$3T+3$	$y^2 = x^6 + (T+1)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 3T + 1$
$2T+1$	$3T+2$	$3T+2$	$y^2 = x^6 + (T+4)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 3T$
$2T+2$	$3T+1$	$3T+1$	$y^2 = x^6 + (T+2)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 3T + 4$
$2T+3$	$3T$	$3T$	$y^2 = x^6 + Tx^5 + 2x^4 + 4x^3 + x^2 + 2x + 3T + 3$
$2T+4$	$3T+4$	$3T+4$	$y^2 = x^6 + (T+3)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 3T + 2$
$3T$	$2T+3$	$2T+3$	$y^2 = x^6 + (4T+1)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 2T + 1$
$3T+1$	$2T+2$	$2T+2$	$y^2 = x^6 + (4T+4)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 2T$
$3T+2$	$2T+1$	$2T+1$	$y^2 = x^6 + (4T+2)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 2T + 4$
$3T+3$	$2T$	$2T$	$y^2 = x^6 + 4Tx^5 + 2x^4 + 4x^3 + x^2 + 2x + 2T + 3$
$3T+4$	2	0	$y^2 = x^6 + 4x^5 + 2Tx^3 + Tx^2 + (T+3)x + 2T + 2$
$3T+4$	$2T+4$	$2T+4$	$y^2 = x^6 + (4T+3)x^5 + 2x^4 + 4x^3 + x^2 + 2x + 2T + 2$
$4T$	$T+3$	$T+3$	$y^2 = x^6 + (2T+1)x^5 + 2x^4 + 4x^3 + x^2 + 2x + T + 1$
$4T+1$	$T+2$	$T+2$	$y^2 = x^6 + (2T+4)x^5 + 2x^4 + 4x^3 + x^2 + 2x + T$
$4T+1$	$4T$	$T+3$	$y^2 = x^6 + 3Tx^5 + Tx^4 + Tx^3 + 2Tx^2 + (T+3)x + T$
$4T+2$	$T+1$	$T+1$	$y^2 = x^6 + (2T+2)x^5 + 2x^4 + 4x^3 + x^2 + 2x + T + 4$
$4T+4$	$T+4$	$T+4$	$y^2 = x^6 + (2T+3)x^5 + 2x^4 + 4x^3 + x^2 + 2x + T + 2$

Example 9.5. Let C_f be the smooth hyperelliptic curve $y^2 = f(x)$ over $\mathbb{F}_7(T)$, where $f(x)$ is one of the polynomials in Table 9.4. Then

$$\mathrm{End}(J(C_f)) = \mathrm{End}_{\mathbb{F}_7(T)}(J(C_f)) = \mathbb{Z}[\eta].$$

Table 9.4. Some curves C over $\mathbb{F}_7(T)$ with $\mathrm{End}(J(C)) = \mathbb{Z}[\eta]$

b	c	d	$C : y^2 = f_{b,c,d}(x)$ reduced modulo 7
0	0	T	$y^2 = x^6 + 2x^4 + (3T+2)x^3 + 5x^2 + 6x + 1$
0	2	T	$y^2 = x^6 + 4x^5 + 3x^4 + 3Tx^3 + 3x^2 + 3x + 1$
0	4	T	$y^2 = x^6 + x^5 + 5x^4 + 3Tx^3 + 2x^2 + 1$
1	0	$5T+4$	$y^2 = x^6 + Tx^4 + 3Tx^3 + (T+1)x^2 + 4x + 5$
3	6	$4T+2$	$y^2 = x^6 + 5x^5 + (T+5)x^4 + Tx^2 + 5x + 6$
4	1	$3T+1$	$y^2 = x^6 + 2x^5 + (T+3)x^4 + 4Tx^3 + Tx^2 + 3$
6	0	$2T$	$y^2 = x^6 + (T+2)x^4 + (T+5)x^3 + Tx^2 + x + 4$
$T+3$	0	4	$y^2 = x^6 + (5T+3)x^4 + 3Tx^2 + 5Tx + 4T + 6$
$3T+3$	$3T$	$6T+6$	$y^2 = x^6 + 6Tx^5 + 2Tx^4 + (2T+4)x^2 + 5T + 6$
$4T+3$	$4T$	$T+6$	$y^2 = x^6 + Tx^5 + 5Tx^4 + (5T+4)x^2 + 2T + 6$
$5T+3$	$5T$	$3T+6$	$y^2 = x^6 + 3Tx^5 + Tx^4 + (T+4)x^2 + 6T + 6$
$6T+3$	$6T$	$5T+6$	$y^2 = x^6 + 5Tx^5 + 4Tx^4 + (4T+4)x^2 + 3T + 6$

Example 9.6. Let C_f be the smooth hyperelliptic curve $y^2 = f(x)$ over $\mathbb{F}_{11}(T)$, where $f(x)$ is one of the polynomials in Table 9.5. Then

$$\mathrm{End}(J(C_f)) = \mathrm{End}_{\mathbb{F}_{11}(T)}(J(C_f)) = \mathbb{Z}[\eta].$$

Table 9.5. Some curves C over $\mathbb{F}_{11}(T)$ with $\mathrm{End}(J(C)) = \mathbb{Z}[\eta]$

b	c	d	$C : y^2 = f_{b,c,d}(x)$ reduced modulo 11
0	0	$T+6$	$y^2 = x^6 + 2x^4 + 7Tx^3 + 5x^2 + 6x + 1$
0	8	$T+9$	$y^2 = x^6 + 5x^5 + 5x^4 + 7Tx^3 + 2x^2 + 1$
5	10	$6T+2$	$y^2 = x^6 + 9x^5 + (T+5)x^4 + Tx^2 + 9x + 10$
$T+5$	0	6	$y^2 = x^6 + (9T+3)x^4 + 10Tx^2 + Tx + 4T + 10$
$2T+5$	$10T$	$7T+10$	$y^2 = x^6 + 9Tx^5 + 9Tx^4 + (9T+8)x^2 + 8T + 10$
$3T+1$	$2T$	$4T+6$	$y^2 = x^6 + 4Tx^5 + 4Tx^4 + 4x^2 + (7T+7)x + T + 5$
$3T+10$	$4T$	$5T+6$	$y^2 = x^6 + 8Tx^5 + 4x^4 + 6Tx^3 + 6x^2 + 5x + T + 8$
$4T+5$	$9T$	$3T+10$	$y^2 = x^6 + 7Tx^5 + 7Tx^4 + (7T+8)x^2 + 5T + 10$

Acknowledgments

I would like to thank my advisor, Yuri Zarhin, for his guidance.

References

[1] W. Bosma, J. Cannon, C. Playoust, *The MAGMA algebra system, I: The user language*. J. Symb. Comp., **24** (1997), 235-265. (See also the MAGMA homepage at `http://www.maths.usyd.edu.au:8000/u/magma/`)

[2] A. Brumer, *The Rank of $J_0(N)$*. Astérisque **228** (1995), 41–68.

[3] C. W. Curtis, I. Reiner, Methods of Representation Theory, Volume 1, John Wiley and Sons, New York, 1981.

[4] J. D. Dixon, B. Mortimer, Permutation Groups, Graduate Texts in Mathematics **163**, Springer-Verlag, Berlin-Heidelberg-New York, 1996.

[5] W. Feit, *The computation of some Schur indices*. Israel J. Math. **46** (1983), 274–300.

[6] D. Gorenstein, Finite Simple Groups, An Introduction to their Classification, Plenum Press, New York and London, 1982.

[7] K. Hashimoto, *On Brumer's family of RM-curves of genus two*. Tohoku Math. J. **52** (2000), 475–488.

[8] T. Ibukiyama, T. Katsura, F. Oort, *Supersingular curves of genus two and class numbers*. Compositio Math. **57** (1986), 127–152.
[9] Yu. I. Manin, *Theory of commutative formal groups over fields of finite characteristic*. Uspehi Mat. Nauk, **18** (1963), 3–90
[10] D. Masser, *Specialization of some hyperelliptic jacobians*. In: Number Theory in Progress (eds. K. Györy, H. Iwaniec, J. Urbanowicz), vol. I, pp. 293–307; de Gruyter, Berlin-New York, 1999.
[11] Sh. Mori, *The endomorphism rings of some abelian varieties*. Japanese J. Math. **2** (1976), 109–130.
[12] Sh. Mori, *The endomorphism rings of some abelian varieties.II*. Japanese J. Math. **3** (1977), 105–109.
[13] B. Mortimer, *The modular permutation representations of the known doubly transitive groups*. Proc. London Math. Soc. (3) **41** (1980), 1–20.
[14] D. Mumford, Abelian varieties, Second edition, Oxford University Press, London, 1974.
[15] N. O. Nygaard, *Slopes of powers of Frobenius on crystalline cohomology*. Ann. Sci. Ecole Norm. Sup. **14** (1981), 369–401.
[16] F. Oort, *Endomorphism Algebras of Abelian Varieties*. Algebraic Geometry and Commutative Algebra (1987), 469–502.
[17] PARI/GP, version `2.1.5`, Bordeaux, 2004, `http://pari.math.u-bordeaux.fr/`.
[18] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, Annals of Mathematics **88** (1968), 492–517.
[19] A. Silverberg, Yu. G. Zarhin, *Variations on a theme of Minkowski and Serre*, J. Pure and Applied Algebra **111** (1996), 285–302.
[20] J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics **106**, Springer-Verlag, New York-Berlin-Heidelberg-Tokyo, 1986.
[21] W. Stein, PARI & MAGMA Calculator, `http://modular.fas.harvard.edu/calc/`.
[22] M.-F. Vignéras, Arithmétique des Algèbres de Quaternions, Lecture Notes in Mathematics **800**, Springer-Verlag, Berlin-Heidelberg-New York, 1980.
[23] J. Wilson, *Explicit moduli for curves of genus* 2 *with real multiplication by* $\mathbb{Q}(\sqrt{5})$, Acta. Arith. **93** (2000), 121–138.
[24] J. Wilson, *Curves of genus* 2 *with real multiplication by a square root of* 5, Oxford University, Ph.D. thesis, 1998.
[25] N. Yui, *On the jacobian varieties of hyperelliptic curves over fields of characteristic* $p > 2$. Journ. of Alg. **52** (1978), 378–410.
[26] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters **7** (2000), 123–132.
[27] Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*. In: Moduli of abelian varieties, (C. Faber, G. van der Geer, F. Oort, eds.), pp. 473–490, Progress in Math., Vol. **195**, Birkhauser, Basel-Boston-Berlin, 2001.
[28] Yu. G. Zarhin, *Very simple* 2*-adic representations and hyperelliptic jacobians*. Moscow Math. J. **2** (2002), issue 2, 403–431.
[29] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication in positive characteristic*, Math. Res. Letters **8** (2001), 429–435.
[30] Yu. G. Zarhin, *Non-supersingular hyperelliptic jacobians*, Bull. Soc. Math. France, **132** (2004) 617–634.

Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA
E-mail address: `arsen@psu.edu`